

2006

Lex-Praxis of Education Informational Privacy for Public Schoolchildren

Susan P. Stuart

Valparaiso University, susan.stuart@valpo.edu

Follow this and additional works at: <https://digitalcommons.unl.edu/nlr>

Recommended Citation

Susan P. Stuart, *Lex-Praxis of Education Informational Privacy for Public Schoolchildren*, 84 Neb. L. Rev. (2005)

Available at: <https://digitalcommons.unl.edu/nlr/vol84/iss4/4>

This Article is brought to you for free and open access by the Law, College of at DigitalCommons@University of Nebraska - Lincoln. It has been accepted for inclusion in Nebraska Law Review by an authorized administrator of DigitalCommons@University of Nebraska - Lincoln.

Lex-Praxis of Education Informational Privacy for Public Schoolchildren

TABLE OF CONTENTS

I. Introduction	1159
II. The Peeping Tom Installs Window Blinds	1162
A. Family Educational Rights and Privacy Act	1162
1. FERPA—The Regime	1164
2. FERPA's Mission Failures	1168
3. FERPA's Textual Problems—Of Athletic Rosters, Class Rings, and Terrorists	1169
B. Protection of Pupils Rights Amendments	1173
C. Individuals with Disabilities Education Act	1176
D. Student Medical Information	1180
1. Medical Records, Generally	1181
2. HIPAA	1182
3. School Nurses	1185
4. Drug and Alcohol Abuse Records	1186
E. Children's Online Privacy Protection Act	1187
F. Government Accountability and Education Statistics	1189
G. Military Recruitment	1191
H. Social Security Numbers	1193
I. School Lunch Programs	1194
III. The Nuts and Bolts: The Protected Information and Its Uses	1195
A. Collection and Maintenance of Government Information	1195
B. Collection and Maintenance of Educational Information	1196
1. Protection of Student-“Owned” Information	1196

© Copyright held by the NEBRASKA LAW REVIEW.

* Associate Professor of Law, Valparaiso University School of Law. B.A., DePauw University; M.Ed., Valparaiso University; J.D., Indiana University-Indianapolis. My many thanks to my hard-working research assistants, Katherine Lord and Lori Marschke.

2. The Scope of Protected Education Information ..	1198
3. Defining Student Permanent Records	1201
C. Acceptable Use of, Access to, and Disclosure of Student Education Information	1203
D. Reformulating Directory Information	1207
IV. "Peaceable Living One Amongst Another": Drafting a Local Policy	1208
A. The Drafters and the Draft	1208
B. The Substance	1210
C. Fair Information Practices	1212
1. Notice/Awareness Principle	1214
2. Choice/Consent Principle	1215
3. Access/Participation Principle	1218
4. Integrity/Security Principle	1219
5. Enforcement/Redress Principle	1223
V. Conclusion	1225

I. INTRODUCTION

Public schools are information-collection machines. Public schools are also the government. Consequently, there is a confluence of concerns about what the government can and should do about protecting the privacy of schoolchildren in that information. Local educational agencies must concern themselves with the legalities of the collection, maintenance, and disclosure of student information, generated both by the agency itself and by the student. Unfortunately, the federal statutes and regulations designed to protect the privacy of that information have run amok.

Regardless of whether the Constitution protects privacy *per se*,¹ most authorities acknowledge the existence of a constitutionally protected privacy interest in personal information following *Whalen v. Roe*.² Indeed, children's informational privacy was at the heart of this decision as several minor plaintiffs challenged the constitutionality of a New York statute that governed the public disclosure of pharmacy records. The statute required the government to collect from pharmacies personal information—names, ages, and addresses—of all indi-

-
1. See generally Susan P. Stuart, *Fun with Dick and Jane and Lawrence: A Primer on Education Privacy*, 88 MARQ. L. REV. 563 (2004). Beyond informational privacy, children should have privacy rights in all aspects of public school life: a constitutional privacy interest should cover the children's workplace as soon as they cross the threshold of school, covering the gamut of confidentiality of grades to prohibition from random videotaping in classrooms.
 2. 429 U.S. 589 (1977). See generally Martin E. Halstuk, *Shielding Private Lives from Prying Eyes: The Escalating Conflict Between Constitutional Privacy and the Accountability Principle of Democracy*, 11 COMMLAW CONSPECTUS 71, 78–80 (2003); Ingrid Schupbach Martin, *The Right to Stay in the Closet: Information Disclosures by Government Officials*, 32 SETON HALL L. REV. 407, 412–23 (2002).

viduals who had obtained certain scheduled, controlled substances by prescription.³ The minor plaintiffs feared public disclosure that would reveal they ingested ritalin to control hyperactivity.⁴ In upholding the statute's constitutionality, the Supreme Court of the United States recognized a "zone of privacy" in information that incorporates two distinct privacy interests, one of which is "the individual interest in avoiding disclosure of personal matters."⁵ The Court determined that the statute did not threaten such privacy interests, in part because the statute properly delineated to government officials a duty not to disclose the information upon pain of prison time, financial penalty, or both. The New York statute therefore properly protected the privacy of information otherwise within the zone of privacy.⁶ In contrast, the crux of the problem with federal statutes that purport to protect student privacy is that these statutes provide for disclosure of and access to student records but provide little affirmative privacy protection.

In the matter of educational information, the government is clearly collecting information from individuals. The vast majority is personal information that is, to a certain extent, given to the government involuntarily because of states' compulsory attendance policies. Following

3. *Whalen*, 429 U.S. at 591-92.

4. *Roe v. Ingraham*, 403 F. Supp. 931, 934 (S.D.N.Y. 1975), *rev'd*, *Whalen v. Roe*, 429 U.S. 589 (1977).

5. *Whalen*, 429 U.S. at 599 (citing Philip P. Kurland, *The Private I*, UNIV. OF CHI. MAG., Autumn 1976, at 7, 8). Although *Whalen v. Roe* has been oft-cited as the progenitor of information privacy, the opinion never really recognized it as such. Only in footnotes did Justice Stevens acknowledge the constitutional underpinnings of privacy arise from, among other places, the Fourteenth Amendment. *Id.* at 598-600 nn.23-26; *see, e.g.*, Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 574-76 (1995). However, most of the United States circuit courts of appeal do recognize a constitutionally protected right to informational privacy. *See Sterling v. Borough of Minersville*, 232 F.3d 190, 195-96 (3d Cir. 2000); *Denius v. Dunlap*, 209 F.3d 944, 955-56 (7th Cir. 2000); *Statharos v. N.Y. City Taxi & Limousine Comm'n*, 198 F.3d 317, 322-23 (2d Cir. 1999); *In re Crawford*, 194 F.3d 954, 958-59 (9th Cir. 1999); *Cantu v. Rocha*, 77 F.3d 795, 806 (5th Cir. 1996); *Eagle v. Morgan*, 88 F.3d 620, 625 (8th Cir. 1996); *Sheets v. Salt Lake County*, 45 F.3d 1383, 1387 (10th Cir. 1995); *Harris v. Thigpen*, 941 F.2d 1495, 1513 (11th Cir. 1991); *Walls v. City of Petersburg*, 894 F.2d 188, 192 (4th Cir. 1990); *Daury v. Smith*, 842 F.2d 9, 13 (1st Cir. 1988); *see also Overstreet v. Lexington-Fayette Urban County Gov't*, 305 F.3d 566, 574 (6th Cir. 2002) (taking a very narrow view of the information that is protected by the constitutional informational privacy). Only the D.C. Circuit absolutely refuses to acknowledge a constitutional right to informational privacy. *See Am. Fed'n of Gov't Employees v. Dept. of Housing & Urban Dev.*, 118 F.3d 786, 793 (D.C. Cir. 1997).

6. *Whalen*, 429 U.S. at 605-06. Similarly, former President Richard M. Nixon was unsuccessful in challenging the Presidential Recordings and Materials Preservation Act, which directed the Administrator of General Services to take custody of Nixon's tapes and papers. The Supreme Court determined, in part, that the General Services' security measures adequately protected the privacy interest involved. *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 458-59, 461-62, 465 (1977).

Whalen v. Roe, then, the government should have a duty not to disclose this information. However, it does not seem to acknowledge such a duty—or at least the federal statutes regulating education informational privacy do not consistently adhere to one. Although the federal statutes and regulations give lip-service to the notion that the information should not be disclosed after collection, the statutes themselves observe that duty more in the breach by the number of “exceptions” it grants to the government to disclose schoolchildren’s personal information. Thus, most handbooks and authorities outlining procedures for local school districts’ privacy policies adhere to the letter of the statutes rather than the rule of constitutionally protected informational privacy.

With *Whalen v. Roe* as its springboard, this Article will focus on schoolchildren’s⁷ rights to informational privacy and will examine the federal statutes that purport to protect that privacy. One root of the problem with education informational privacy is the systemic failure of the numerous—and rather uncoordinated—federal statutes to recognize a *per se* privacy right or liberty in schoolchildren. Another problem is that the current legislation projects several privacy goals, yet sets out no clearly articulated privacy interest at all, at least no clearly articulated interest in the schoolchildren themselves. Instead, the statutes are a hodgepodge of piecemeal legislation that protects very little informational privacy for children. As a result, local educational agencies, who must implement the protections, are left to their own devices to untangle the incoherency of the statutory privacy “protections” for their constituent children and determine exactly what they can and cannot do with their information.⁸

7. This Article will confine itself to privacy for children not yet graduated from high school. Some matters raised here may be applicable to students in postsecondary educational institutions, but the vast majority of the pertinent statutes deal with minors, or children under the age of eighteen.

8. The United States Department of Education recently published guidelines for state and local agencies to follow in formulating privacy policies. NAT’L FORUM ON EDUC. STATISTICS, U.S. DEP’T OF EDUC., FORUM GUIDE TO PROTECTING THE PRIVACY OF STUDENT INFORMATION: STATE AND LOCAL EDUCATION AGENCIES (2004), available at <http://nces.ed.gov/pubs2004/2004330.pdf> [hereinafter FORUM GUIDE]. This *Forum Guide* is quite comprehensive and thoughtful. However, it still relies on, and therefore suffers from, the underlying, incorrect assumption that the relevant federal laws and regulations actually protect the privacy of education information. The *Forum Guide* is a guide to statutes, not an analytical compendium of student privacy interests. It merely builds on previous work that had explained the Family Educational Rights and Privacy Act, then tacks on “new laws affecting the privacy issue . . . and more guidelines . . . provided by the U.S. Department of Education and the U.S. Department of Agriculture.” *Id.* at vii. Thus, when the *Forum Guide* asserts that “[f]ederal and state privacy statutes pertaining to students build on the concept of common law and constitutional provisions that imply privacy guarantees,” *id.* at 1, one must be skeptical about the legal analysis involved.

Starting with the premise that students' informational privacy is constitutionally protected, this Article will examine the federal statutes that purport to protect that privacy.⁹ Part II will sort through the current versions of federal statutes that regulate the collection, maintenance, and disclosure of student information and examine whether they actually protect student privacy interests. Part III will outline what information a local policy must constitutionally protect that the statutes really do not. Finally, Part IV will set out a plan for incorporating fair information practices into the framework of any local privacy policy and thereby set out a more coherent praxis for school administrators to follow, one that will comply, at the very least, with the same informational privacy standards that are afforded adults.

II. THE PEEPING TOM INSTALLS WINDOW BLINDS¹⁰

As one sorts through the federal legislation that touches on schoolchildren's informational privacy, one must keep reminding oneself that there is a per se constitutionally protected privacy right in personal information because the statutes themselves are not entirely clear that privacy is the goal or that they are actually offering any protections at all. Almost every statutory scheme intended to protect schoolchildren's privacy is replete with incongruities and problems that, if followed, put local schools in violation of the clearly articulated constitutional right to informational privacy.

A. Family Educational Rights and Privacy Act

The worst offender in the constitutional-violation derby is the Family Educational Rights and Privacy Act ("FERPA")¹¹—also known as the "Buckley Amendment"—which has long been considered the gold standard for protecting education privacy.¹² FERPA was enacted

9. State statutes are equally important to consider here, especially constitutional privacy provisions. See, e.g., Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1420–31. However, their treatment is beyond the scope of this Article. See generally Susan P. Stuart, *A Local Distinction: State Education Privacy Laws for Public Schoolchildren*, 108 W. VA. L. REV. (forthcoming 2006).

10. "Relying on the government to protect your privacy is like asking a peeping tom to install your window blinds." John Perry Barlow, *Decrypting the Puzzle Palace*, COMM. OF THE ACM, July 1992, at 25, 26, available at <http://portal.acm.org/citation.cfm?id=129910&coll=ACM&dl=ACM&CFID=68402275&CFTOKEN=24466185>.

11. 20 U.S.C. § 1232g (Supp. II 2002).

12. *Id.* For two related articles that are invaluable resources for picking through the morass that is FERPA, see Lynn M. Daggett & Dixie Snow Huefner, *Recognizing Schools' Legitimate Educational Interests: Rethinking FERPA's Approach to the Confidentiality of Student Discipline and Classroom Records*, 51 AM. U. L. REV. 1 (2001); Lynn M. Daggett, *Bucking Up Buckley I: Making the Federal Student*

in 1974, ostensibly to protect children's informational privacy. Aside from the fact that its privacy protection has been oversold because it is just too confusing, the Supreme Court recently held, in *Gonzaga University v. Doe*,¹³ that FERPA confers no explicit enforceable right for a violation.¹⁴ In so doing, the Court essentially eviscerated FERPA's protection for children's informational privacy in. Today, the only real penalty for violating a student's informational privacy right is that the United States Department of Education ("DOE") can penalize an educational agency if it has a "policy or practice"¹⁵ of disclosing education records or of denying parental access to those records.¹⁶ That leaves for consideration exactly how much juice remains in FERPA, if any.

Records Statute Work, 46 CATH. U. L. REV. 617 (1997) [hereinafter Daggett, *Buckley* I].

13. 536 U.S. 273 (2002).

14. *Id.* at 287. In *Gonzaga University*, a former student sued Gonzaga University for a violation of FERPA after a university administrator reported to the State of Washington's teacher certification board that the plaintiff had allegedly engaged in sexual misconduct. *Id.* at 277. The Court held that Congress had not included any rights-creating language in FERPA's nondisclosure provisions and therefore had not created a private right of action for a FERPA violation. *Id.* at 287. FERPA may not be enforceable via § 1983 either. *Taylor v. Vt. Dept. of Educ.*, 313 F.3d 768, 783-85 (2d Cir. 2002); *Combiar v. Biegelsen*, No. 03 CV 10304(GBD), 2005 WL 477628, at *5 (S.D.N.Y. Feb. 28, 2005). *But see* *Ashby v. Isle of Wight County Sch. Bd.*, 354 F. Supp. 2d 616 (E.D. Va. 2004). Instead, an educational agency's violation of FERPA may only be penalized by loss of federal funding through DOE enforcement. *Gonzaga University*, 536 U.S. at 290; *see also* *Shockley v. Svodoba*, 342 F.3d 736, 741 (7th Cir. 2003); *D.L. v. Unified Sch. Dist. # 497*, 270 F. Supp. 2d 1217, 1244 (D. Kan. 2002) (relying, in part, on *Gonzaga University* to justify ordering a school to comply with a discovery request for the names and addresses of non-party students because the school would not suffer any liability under FERPA so long as the parents were notified by the school), *amended by* No. 00-2439-CM, 2002 WL 31296445 (D. Kan. 2002), *modified*, No. 00-2439-CM, 2002 WL 31253740 (D. Kan. 2002), *vacated on other grounds*, 392 F.3d 1223 (10th Cir. 2004). In any event, no reported cases to date indicate that any school district has lost federal funds for having violated FERPA. Not only do students not have any personally enforceable rights of nondisclosure, parents do not have an enforceable right to access. *See Taylor*, 313 F.3d at 783-85; *see also* *J.P. ex rel. Popson v. W. Clark Cmty. Sch.*, 230 F. Supp. 2d 910, 948-49 (S.D. Ind. 2002) (indicating that FERPA does not create a private right of action for parents to contest the destruction of education records).

15. A single instance of improper and deliberate disclosure does not make a violation. For example, providing student records pursuant to a single discovery request may not be a policy or practice in violation of FERPA. *E.g.*, *Ellis v. Cleveland Mun. Sch. Dist.*, 309 F. Supp. 2d 1019, 1023-24 (N.D. Ohio 2004).

16. *E.g.*, *id.* at 1023. Except insofar as there is an enforcement mechanism through the DOE's Family Policy Compliance Office ("FPCO"), a parent may have little recourse to view her child's records. 34 C.F.R. § 99.63 (2005). The Student Privacy Protection Act of 2003 was introduced in the House as House Report 1848 on April 29, 2003, and would provide a private remedy for a violation of FERPA. Both injunctive and monetary relief are specified with treble damages for willful or knowing violations. *Id.* There seems to be no immediate movement toward this Act's passage.

1. FERPA—The Regime

It should never be assumed that FERPA protects informational privacy. FERPA follows, to a limited extent, the formatting of adult privacy statutes that regulate certain data-gathering practices and disclosures and that limit access to private, personally identifiable information. However, for reasons that are inexplicable, the children's privacy protections in FERPA are not co-extensive with the protections afforded to adults whose private information is held by the government. In addition, FERPA is an incoherent maze of legislative double-talk, making it difficult to determine what are protected "education records" and what are not, or who can have access and who cannot.¹⁷ What is clear is that FERPA grants certain rights to parents and "eligible" students over the age of seventeen¹⁸ but no *privacy* rights to children under the age of eighteen.

FERPA's structure has two basic parts: the information that is protected, and the practices to regulate and protect that information. First, the information that is subject to FERPA's regulation and protection consists of "education records." "Education records" are "records, files, documents, and other materials which . . . contain information directly related to a student; and . . . are maintained by an educational agency or institution or by a person acting for such agency or institution."¹⁹ FERPA's designation of what constitutes "education records" hardly merits much criticism, except for its brevity, lack of clarity, and some confusion about the applicable agency regulations—a "sin of omission." The bigger problem with FERPA is in its so-called privacy practices and procedures—a "sin of commission."

Second, the regulatory framework for FERPA provides four basic categories of what might be considered "fair information practices"²⁰ for those records. These categories are: (i) providing access to educa-

17. For example, congressional language is difficult to interpret in the following: one of FERPA's exemptions to prohibiting nonconsensual disclosure of information is a disclosure to "other school officials, *including* teachers within the education institution or local educational agency, who have been determined by such agency or institution to have legitimate educational interests, *including* the educational interest of the child for whom consent would otherwise be required." 20 U.S.C. § 1232g(b)(1) (Supp. II 2002) (emphasis added). Any reviewer of the rules of statutory interpretation would be hard-pressed to interpret who is "included" in this exemption. The maze of FERPA regulations is equally difficult to navigate. See *generally* 34 C.F.R. pt. 99.

18. 20 U.S.C. § 1232g(d).

19. *Id.* § 1232g(a)(4)(A). FERPA also lists information not considered education records, such as work-product of educational personnel, records maintained by any police agency of the institution, and records of students over the age of seventeen. *Id.* § 1232g(a)(4)(B). These sources may still be constitutionally protected information; FERPA just does not regulate them.

20. See *infra* notes 53–54.

tional records to parents;²¹ (ii) providing notice of access and rights to parents;²² (iii) prohibiting disclosure of school records;²³ and (iv) regulating the collection of information.²⁴ There are no penalties for a violation of the last practice;²⁵ thus, only the first three practices have any viable protection under FERPA.

With regard to the first privacy practice, FERPA's right of access inures only to parents and gives them the right to inspect and review their children's education records.²⁶ A school must also give parents the opportunity to challenge the content of the education records: to delete or change inaccurate, misleading, and other information that otherwise violates the "privacy rights" of the student.²⁷ There is no right to free copies of the records, but there is a right to have the records interpreted.²⁸

Related to its second information practice of access is FERPA's mandate that local educational agencies provide annual notice to parents of currently enrolled students of FERPA's policies and practices.²⁹ Indeed, this notice must "effectively" inform parents of their FERPA rights.³⁰ The notice must alert the recipients to their right to inspect and review their children's educational records, their right to challenge and amend those records, their right to consent to release those records (if not otherwise presumed under the Act), and their right to file a complaint with DOE.³¹ The notice must also provide the content of directory information, as discussed below; the school's intent to regularly disclose without permission; and the process for objecting to such disclosure. That type of disclosure is one of several that is problematic under FERPA.

Third, and presumably the privacy centerpieces for FERPA, are the information practices intended to prohibit disclosure, and thereby maintain the confidentiality of education records. Actually, the infor-

21. 20 U.S.C. § 1232g(a)(1)(A).

22. *Id.* § 1232g(e).

23. *Id.* § 1232g(b)(1).

24. *Id.* § 1232g(c).

25. Compare *id.* § 1232g(a)(1)(A), and *id.* § 1232g(b)(1), with *id.* § 1232g(c). The fourth information practice, which limits data-gathering, is more directed to family privacy than to students' informational privacy and thus has less significance for purposes of regulating education informational privacy per se to which FERPA ostensibly is directed. However, its family privacy theme is refined in and reframed by the Protection of Pupil Rights Amendments as an education privacy issue. See *infra* notes 65–78.

26. 20 U.S.C. § 1232g(a)(4)(B); 34 C.F.R. § 99.10 (2005).

27. 34 C.F.R. § 99.20.

28. *Id.* §§ 99.10–12; Daggett, *Buckley I*, *supra* note 12, at 629–30.

29. FERPA regulations used to require a written student-records policy. See Daggett, *Buckley I*, *supra* note 12, at 639.

30. 20 U.S.C. § 1232g(e). This notice requirement also applies to eighteen-year-old students who are "eligible." *Id.*; see *infra* text accompanying note 50.

31. 34 C.F.R. § 99.7.

mation itself is not protected by the statute. Instead, an educational institution can be financially penalized for a "policy or practice" of releasing education records or "personally identifiable information"³² without written *parental* consent.³³ Such parental consent must specify personally identifiable information from student records and must specify "the records to be released, the reasons for such release, and to whom, and with a copy of the records to be released to the student's parents and the student if desired by the parents."³⁴

But there is also a carve-out exception to the "personally identifiable information" category of student information that a local educational agency may disclose without permission. "Directory information"³⁵ is outside the purview of the nondisclosure provisions of FERPA and can be released without parental consent.³⁶ Directory information includes

the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent education agency or institution attended by the student.³⁷

In order to effectuate nonconsensual disclosure of such information, the educational agency must make public a notice of which information it considers "directory information," thus affording parents the opportunity to opt out of such disclosure by objecting to the release of some or all of the information.³⁸ The typical use of such information is intended to be limited to such intrascholastic uses as the publication of school yearbooks, honor rolls, sports programs, and playbills.

In addition, FERPA's third information practice approves certain disclosures of education records for which parental consent is presumed not to be required. Most of these nonconsensual disclosures are related to the educational function of the institution, such as disclosures within the institution itself for "legitimate educational interests,"³⁹ disclosures to other education agencies from which the student may be seeking services,⁴⁰ disclosures to federal and state authorities for auditing and evaluating,⁴¹ disclosures in applications for

32. *Id.* § 99.3.

33. 20 U.S.C. § 1232g(b)(1). This written consent must designate which records can be released and to whom. Daggett, *Buckley I*, *supra* note 12, at 631.

34. 20 U.S.C. § 1232g(b)(2); 34 C.F.R. § 99.30. FERPA's regulations were recently amended to allow for electronic consent. *Id.*

35. 20 U.S.C. § 1232g(a)(5)(A).

36. 34 C.F.R. § 99.31.

37. 20 U.S.C. § 1232g(a)(5)(A); *see also* 34 C.F.R. § 99.3.

38. 20 U.S.C. § 1232g(a)(5)(B).

39. *Id.* § 1232g(b)(1)(A).

40. *Id.* § 1232g(b)(1)(B).

41. *Id.* § 1232g(b)(1)(C).

financial aid,⁴² and disclosures for testing and instructional improvement.⁴³ Schools must maintain written logs of actual access as well as denial of requests for access.⁴⁴ And there is a prohibition on tertiary disclosure: if personally identifiable information is disclosed to one party, then there is to be no further disclosure by that party.⁴⁵

Among the categories of nonconsensual disclosure approved by FERPA—but which merits a bit more examination—is disclosure outside the ordinary educational use of student records to authorities in the criminal justice system. First, FERPA affords access to juvenile justice authorities as governed by state laws that allow such reporting or disclosure and that require written assurance of confidentiality of those records, except upon written consent of the parent.⁴⁶ Second, education records are subject to federal grand jury and other law enforcement subpoenas served upon the educational agencies.⁴⁷ This latter type of disclosure particularly contrasts with FERPA's limitation on disclosure and access to personally identifiable information in education records under *other* judicial orders or subpoenas, for which the educational agency must notify the parents and the students before compliance.⁴⁸

42. *Id.* § 1232g(b)(1)(D).

43. *Id.* § 1232g(b)(1)(F).

44. *Id.* § 1232g(b)(4)(A); 34 C.F.R. § 99.32 (2005).

45. 20 U.S.C. § 1232g(b)(4)(B); 34 C.F.R. § 99.33. The regulations do allow further tertiary disclosures if they are within the recognized exceptions for nonconsensual disclosure. *Id.* §§ 99.31, .33(b).

46. 20 U.S.C. § 1232g(b)(1)(E).

47. *Id.* § 1232g(b)(1)(J). The contents of those subpoenas and the records disclosed may be “sealed” for “good cause.” *Id.*; see also Daggett, *Buckley I*, *supra* note 12, at 634–35 (“In the case of law enforcement subpoenas, the new language now states that for good cause, the issuing court shall or may order the school not to disclose the existence or the contents of the subpoena or the records released pursuant to the subpoena.”).

48. 20 U.S.C. § 1232g(b)(2)(B). On a related note, *Gonzaga University* may have made these law enforcement provisions unenforceable. If FERPA affords no enforceable right of privacy in students then it likely provides no right of access to student records by parents. *Taylor v. Vt. Dept. of Educ.*, 313 F.3d 768, 783–85 (2d Cir. 2002); see also *J.P. ex rel. Popson v. W. Clark Cmty. Sch.*, 230 F. Supp. 2d 910, 948–49 (S.D. Ind. 2002) (citing the Supreme Court’s holding in *Gonzaga University* for the proposition that FERPA does not show congressional intent sufficient to create this parental right). And if FERPA provides no right of access to parents, then third-party access is likely not enforceable either. So in a roundabout way, *Gonzaga University* may have protected education privacy rights, at least with regard to tertiary disclosure.

In a new development applicable to access under FERPA, on January 4, 2005, House Report 81 was introduced to provide crime victims with access to records at postsecondary institutions. See generally Maureen P. Rada, Note, *The Buckley Conspiracy: How Congress Authorized the Cover-Up of Campus Crime and How It Can Be Undone*, 59 OHIO ST. L.J. 1799 (1998) (arguing that FERPA must be amended so that FERPA’s “educational records” do not include disciplinary records and that those records must be affirmatively disclosed by institutions of

2. FERPA's Mission Failures⁴⁹

The overarching general concern with FERPA is that it genuinely has no application to children's privacy interests whatsoever. Nowhere in the text nor in the mission of FERPA is the recognition that this education information—records, personally identifiable information, and directory information—belongs to the students or that children may have an individual privacy interest in the collection, maintenance, and disclosure of that information separate from their parents and the educational agencies.

FERPA's first mission—"Family Educational Rights"—has little or no significance to the regulated students themselves. For instance, the information practice concerning access to student information articulates parental rights to access the records of students, but none for a student until she or he becomes an "eligible student" upon turning eighteen.⁵⁰ Indeed, FERPA assumes a paternalistic attitude toward the ability of children to exercise their autonomy that is not mirrored in other privacy statutes.⁵¹ Perhaps parents are given this empowerment for the purpose of protecting their children's interests in limiting government collection of data and in assuring that such data is accurate, thus ensuring family privacy. But what is strikingly anomalous is that, except for a backhanded reference in a regulation,⁵² students have no privacy rights in accessing that information themselves, while a similarly regulated group of government constituents—*adult* federal employees—has an explicit right of access to their own information under the Privacy Act of 1974.⁵³ Obviously, children of tender years

higher education); Ethan M. Rosenzweig, Note, *Please Don't Tell: The Question of Confidentiality in Student Disciplinary Records Under FERPA and the Crime Awareness and Campus Security Act*, 51 EMORY L.J. 447 (2002); Benjamin F. Sidbury, Note, *The Disclosure of Campus Crime: How Colleges and Universities Continue to Hide Behind the 1998 Amendment to FERPA and How Congress Can Eliminate the Loophole*, 26 J.C. & U.L. 755 (2000).

49. The most obvious failing of FERPA is, of course, that it is not privately enforceable either on its own or via § 1983. See *supra* notes 13–16. Institutional funding penalties are so unlikely—extensive research unearthed no cases involving such penalty—that it is hard to say why any school district even pays any attention to FERPA.
50. 20 U.S.C. § 1232g(d); 34 C.F.R. §§ 99.3, .5; Daggett & Huefner, *supra* note 12, at 6. However, one FERPA regulation, although not the statute itself, does allow for disclosure to the student. See 34 C.F.R. § 99.31(a)(12).
51. Other privacy statutes include "minors" among those who may exercise their "rights" thereunder. See Anita L. Allen, *Minor Distractions: Children, Privacy and e-Commerce*, 38 HOUS. L. REV. 751, 759, 774–75 (2001). Anita Allen cites to minors' privacy rights as protected under the Privacy Act of 1974, the Fair Credit Reporting Act, the Right to Financial Privacy Act, the Video Privacy Protection Act, and the Employee Polygraph Protection Act. *Id.* at 774 n.143.
52. See 34 C.F.R. § 99.31(a)(12).
53. 5 U.S.C. § 552a(d) (2000) ("Each agency that maintains a system of records shall . . . upon request by any individual to gain access to his record or to any informa-

likely have no intrinsic interest in their education records so granting a blanket right of access to the actual "owners" of the records might seem foolish, even unwise. However, there seems to be no compelling reason to overlook entirely the interests of the true stakeholder in the records, especially as the stakeholder becomes more mature and is assumed to have the intellectual capacity to make decisions on her own.

The second part of the congressional mission of FERPA—"Privacy Act"—purports to protect privacy but is better characterized as a framework for fair information practices, a statutory framework that regulates the dissemination of government records. Unfortunately, that framework evinces little recognition that those records are the cumulative work-product of students and are not traditional "employment" records.⁵⁴ Until they are eighteen, students do not have the power of consent over the disclosure of their records; their parents do. Indeed, the only "power" granted to students over disclosure of their own records is in one of FERPA's regulations, which allows disclosure to students of their own records as an exception to the prior parental consent requirement!⁵⁵ The practical effect of FERPA then, is to marginalize children's privacy rights in matters that are personally their own. Thus, a local educational agency's compliance with FERPA's framework in protecting children's privacy is a risky option at best if, indeed, children have their own articulable constitutional right to informational privacy as *Whalen v. Roe* suggests.

3. FERPA's Textual Problems—Of Athletic Rosters, Class Rings, and Terrorists

FERPA contains two major textual problems that fly in the face of students' constitutional informational privacy. The first deals with the nearly uncontrolled, nonconsensual use of students' personally identifiable information that FERPA denominates as "directory information." The second, and more recent problem, deals with the non-consensual disclosure of similar information for anti-terrorism purposes.

The first major textual problem in FERPA is its treatment of students' directory information and its nonconsensual disclosure. The confusing statutory language concerning directory information gives no right to schools to release that information without consent; there

tion pertaining to him which is contained in the system, *permit him* and upon his request, a person of his own choosing to accompany him, *to review the record* and have a copy made of all or any portion thereof in a form comprehensible to him.") (emphasis added).

54. Such "ownership" by the students is implicitly recognized in the automatic transfer of education records when a child changes schools. 20 U.S.C. § 1232g(b)(1)(B).

55. 34 C.F.R. § 99.31(a)(12) ("The disclosure is to the parent of a student who is not an eligible student or *to the student.*") (emphasis added).

is no affirmative mandate nor privilege in FERPA for schools to disseminate this information. Instead, the statutory language presupposes that educational agencies have the right to release directory information, by penalizing disclosure of personally identifiable information that is *not* "directory information."⁵⁶ Perhaps Congress deemed such dissemination of directory information a "routine use," defined by the Privacy Act of 1974 as "the use of such record for a purpose which is compatible with the purpose for which it was collected."⁵⁷ However, even the Privacy Act contains no such "routine use" of adult information as is presumed under FERPA, which provides no statutory protection of directory information as protected education records.

Chiefly problematic is the character of the information that FERPA considers to be directory information. Among the items set forth as directory information are certain vital statistics about the students as children and about their families. It is critical that the local educational agency collect this information under its government recordkeeping duties, in order to complete government reports for attendance, finance, and testing. These vital statistics and familial information are also essential for undertaking in loco parentis obligations for the health, care, and welfare of an agency's minor charges. Thus, these records are collected for the government uses, school *qua* government.

But there is also information that FERPA deems directory information that is collected and maintained for a school's other function, school *qua* educational agency. Such information includes a student's major field of study, attendance dates, grade level, athletic participation, and the like. This information is generated by the child as student as a record of her educational work-product and not just as a vital statistic intended to keep the school's governmental function running smoothly.

Thus, directory information is collected for both governmental and educational purposes but, under FERPA, can be routinely disclosed regardless of the "purpose for which it was collected." And FERPA contains very few controls over the dissemination of this peculiarly personal information—including addresses, phone numbers, e-mail addresses, and photographs—to be shared nonconsensually with nonrelated third parties. Worse, the DOE itself has clouded the problem.⁵⁸ The DOE's guidance for local educational agencies allows for

56. 20 U.S.C. § 1232g(b)(1), (2).

57. *Id.* § 552a(a)(7). The language of the Privacy Act of 1974 specifically allows limited "routine use" of government-collected information. *Id.*

58. For example, the DOE's regulation that sets out the protocols for the use of directory information exceeds—although not by a great measure—the authorization of FERPA. According to the regulation,

release of directory information in circumstances that would be considered unlawful under adult privacy statutes. Functionally, the DOE has merged all the collected information into a single category, treating both governmentally and educationally collected information as one and the same, and all directory information can be routinely disclosed without consent for intrascholastic disclosure in school publications and extrascholastic disclosure to outside commercial organizations.⁵⁹

The first type of nonconsensual disclosure to intrascholastic publications is obviously within the educational mission of the institution. Schools should be able to elect to distribute certain directory information for school functions, such as programs for dramatic productions and musicals, school yearbooks, honor rolls, graduation programs, and sporting event rosters. This type of nonconsensual disclosure certainly seems a "routine educational use," a use for which the information was originally gathered. Although routine use disclosure of some of this personal information is probably outside the educational-function gathering—a student's address, telephone number, and the like—the remaining information typically is confined to intrascholastic disclosure and under circumstances that clearly have something to do with the educational mission of the school. It makes good sense that a school need not get consent every single time a child's basketball scoring prowess is mentioned in the local newspaper.

However, the DOE's second authorized routine use is problematic because it allows nonconsensual disclosure of students' directory information to commercial companies.⁶⁰ There is some attraction to the

"[d]irectory information" means information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed. It includes, but is not limited to, the student's name, address, telephone listing, electronic mail address, photograph, date and place of birth, major field of study, dates of attendance, grade level, enrollment status (e.g., undergraduate or graduate, full-time or part-time), participation in officially recognized activities and sports, weight and height of members of athletic teams, degrees, honors and awards received, and the most recent education agency or institution attended.

34 C.F.R. § 99.3 (emphasis added).

59. These functions are not within either FERPA or its regulations but are extrapolated from the *Model Notice* provided by the DOE for school administrators to use as a notice to parents. U.S. DEP'T OF EDUC., MODEL NOTICE FOR DIRECTORY INFORMATION, <http://www.ed.gov/policy/gen/guid/fpc/ferpa/mndirectoryinfo.html> (last visited May 15, 2006) [hereinafter MODEL NOTICE]. There is a third nonconsensual disclosure mentioned in the guidance: military access to student lists. Such access is not afforded by FERPA but is afforded by other statutes. See *infra* notes 169–83.
60. MODEL NOTICE, *supra* note 59. The DOE model guidance for nonconsensual disclosure does not limit the commercial enterprises that might receive rolls of this information although the nonexclusive list is limited to vendors of student-oriented paraphernalia, such as class rings and yearbooks.

notion that the dissemination of this information to outside organizations—such as address and telephone lists—has a limited and minimal educational function when those companies manufacture student-oriented items like class rings or publish yearbooks. However, such disclosure has a significantly more attenuated educational function than intrascholastic publication as more a matter of business convenience than of educational concern. Such disclosure is also subject to significant abuse as these lists of students can generate a great deal of money as marketing lists.⁶¹ And because directory information is outside FERPA's protections and prohibitions, nothing limits these tertiary users from redistributing or selling the lists to other commercial entities that are not educationally related.⁶²

The second major textual problem in FERPA was added in 2001, via the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA Patriot Act"),⁶³ which amended FERPA to add a provision to assist in the investigation and prosecution of terrorism.⁶⁴ This provision al-

61. A chief complaint by adults about government distribution of this type of directory information, such as that derived from the rolls of the Bureau of Motor Vehicles, is that its sale generates a lot of revenue for the state. *See, e.g., Reno v. Condon*, 528 U.S. 141, 143 (2000) (upholding the Driver's Privacy Protection Act of 1994 as a proper exercise of Congress's Commerce Clause powers). Student profiling is also big business. Companies can do an end-run around privacy issues by collecting identifiable information from students under the guise of serving college admissions departments. Instead, the companies sell the information to direct marketers and other commercial concerns. *See, e.g., Fed. Trade Comm'n, High School Student Survey Companies Settle FTC Charges*, <http://www.ftc.gov/opa/2002/10/student1r.htm> (last visited May 15, 2006); Electronic Privacy Information Center, *Privacy and Consumer Profiling*, <http://www.epic.org/privacy/profiling> (last visited May 15, 2006) (defining consumer profiling as the aggregation of information that can be compiled to reveal buying and spending habits and the creation of dossiers that can be sold to commercial enterprises). There is a lot of money to be made from student lists. For example, lists of middle school students—ages eleven to thirteen—go from \$70 per 1000 for a one-time use, to \$250 per 1000 of e-mail addresses one-time use. *See, e.g., Student Marketing Group, Junior High, Middle School Database*, http://www.studentmarketing.net/junior_pop.htm (last visited May 15, 2006). Student profiling also raises concerns about manipulation. LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* 153–54 (1999).

62. In contrast, the Privacy Act of 1974 forbids the sale of names and addresses by agencies unless specifically authorized by law. 5 U.S.C. § 552a(n) (2000).

63. Pub. L. No. 107-56, 115 Stat. 272 (2001).

64. 20 U.S.C. § 1232g(j) (Supp. II 2002); *see also* USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272. This new FERPA provision, passed as part of the USA Patriot Act, is likely enforceable, unlike the remainder of FERPA after *Gonzaga University*. Unlike FERPA, the USA Patriot Act was not enacted under Congress's spending powers. Thus, the USA Patriot Act significantly weakened not only some overall notions of privacy but several specific privacy statutes as well, such as FERPA. Marc Rotenberg, *Foreward: Privacy and Secrecy After September 11*, 86 MINN. L. REV. 1115, 1118 & n.15 (2002).

lows federal officers, with the authority of an Assistant Attorney General, to seek an ex parte order for the collection of education records that are "relevant to an authorized investigation or prosecution of an offense listed in section 2332b(g)(5)(B) of Title 18 [the USA Patriot Act], or an act of domestic or international terrorism as defined in section 2331 of that title."⁶⁵ Although this provision requires the user to keep the information confidential, the greater horror is the nearly nonexistent due process standard for requesting a court order: "specific and articulable facts giving reason to believe that the education records are likely to contain information described in paragraph (1)(A)."⁶⁶ Thus, the USA Patriot Act made disclosure of educational records a matter of routine if they might be relevant.⁶⁷ In so doing, Congress exposed children's private information to seizure without the typical statutory privacy protections that would incorporate "a wide range of Fourth Amendment values, such as an articulated probable cause standard, a notification requirement, a nexus between the authority granted and the area searched, and means of judicial oversight."⁶⁸ This new textual problem just adds to the headache of any local educational agency trying to protect students' informational privacy when trying to comply with FERPA.

B. Protection of Pupils Rights Amendments

Contiguous to FERPA is the Hatch Act, or the Protection of Pupils Rights Amendment ("PPRA").⁶⁹ PPRA expanded on the earlier language of 20 U.S.C. § 1232h⁷⁰ to purportedly create a set of "pupil

65. 20 U.S.C. § 1232g(j).

66. *Id.* § 1232g(j)(2).

67. John W. Whitehead & Steven H. Aden, *Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the USA Patriot Act and the Justice Department's Anti-terrorism Initiatives*, 51 AM. U. L. REV. 1081, 1132 (2002).

68. Rotenberg, *supra* note 64, at 1117.

69. 20 U.S.C. § 1232h (originally enacted as Goals 2000: Educate America Act, Pub. L. No. 103-227, § 1017, 108 Stat. 125, 268 (1994)); *see also* 34 C.F.R. pt. 98 (2005). This portion of the General Education Provisions Act was the original goal envisioned by the "privacy" movement impelling passage of FERPA in 1974. PPRA directly addresses those concerns in limiting the perceived intrusive data-collection practices by schools. *See, e.g.*, THE PRIVACY PROT. STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 419-20 (1977) [hereinafter PRIVACY REPORT]; Margaret L. O'Donnell, *FERPA: Only a Piece of the Privacy Puzzle*, 29 J.C. & U.L. 679, 684-85 (2003).

70. An earlier version of 20 U.S.C. § 1232h was devoted to parental rights to inspect instructional material and, as an adjunct to family—but not necessarily student—privacy rights, to the right not to be asked certain "personal" questions in the administration of psychiatric and psychological research instruments in the classroom. Education Amendments of 1974, Pub. L. No. 93-380, § 514(a), 88 Stat. 484, 574, *amended by* Education Amendments of 1978, Pub. L. No. 95-561, § 1250, 92 Stat. 2355-56; *see also* Daggett, *Buckley I*, *supra* note 12, at 650.

rights" that have some tangential relevance to student privacy. In reality, PPRA has nothing to do with pupil rights but is rather a euphemism for parental control over children—perhaps, "family" privacy—and over the educational process. Instead of creating anything that resembles a right of privacy in the individual student, PPRA enacted: (i) a parental right to inspect instructional materials; (ii) a parental consent requirement for minor students to participate in any research program that might reveal certain "personal" information;⁷¹ and (iii) a mandate to local educational agencies to develop, in concert with parents, policies concerning student privacy, parental access to information, and the administration of physical examinations to students. Like FERPA, PPRA requires annual notification of these policies—reasonable notice—directly to parents with the opportunity for parents to opt out of the listed activities.⁷² Thus, PPRA empowers parents and requires educational agencies to formulate policies that reflect that parental empowerment. However, PPRA does not do much more than has anything to do with its avowed and titular purpose: "pupil rights."

Because of the absence of rights-creating language and because PPRA too was passed under the spending powers of Congress, PPRA likely has no enforceable rights like FERPA.⁷³ Despite recent efforts, there is no explicit private right of action in this statute.⁷⁴ Regardless, the enforcement penalties under PPRA for loss of funding are much more ephemeral than under FERPA: "The Secretary shall take such action as the Secretary determines appropriate to enforce this

Other amendments to PPRA were in the No Child Left Behind Act of 2001, Pub. L. No. 107-110, § 1061, 115 Stat. 1425, 2083.

71. The categories of such information deemed private have more to do with family control over their children's activities, nominally family "privacy," than with individual students' privacy. See, e.g., *C.N. v. Ridgewood Bd. of Educ.*, 319 F. Supp. 2d 483, 498 (D.N.J. 2004) (discussing the types of information that warrant protection in the context of the family and the student), *aff'd*, 430 F.3d 159 (3d Cir. 2005). In *C.N.*, the district court held that the disclosure of highly personal information by students, during the course of a voluntary and anonymous survey of at-risk behaviors, was not a violation of any constitutional right of privacy in the child, nor a violation of any so-called right to family privacy. *Id.* at 496-98. The facts indicate that the administering school district had actually complied—for the most part—with PPRA.
72. 20 U.S.C. § 1232h(c)(2).
73. The current version of PPRA was in Goals 2000: Educate America Act, an appropriations bill for all federally funded education programs and for education reform. Pub. L. No. 103-227, § 1017, 108 Stat. 125, 268 (1994).
74. *C.N. v. Ridgewood Bd. of Educ.*, 146 F. Supp. 2d 528, 535 & n.7, *aff'd in part, rev'd in part on other grounds*, 281 F.3d 219 (3d Cir. 2001); cf. *C.N.*, 319 F. Supp. 2d at 489 (observing that *Gonzaga University* was the impetus for the stipulated dismissal of FERPA and PPRA claims concerning student surveys that sought information about at-risk behaviors).

section,"⁷⁵ and only an educational agency's utter failure to comply on a long-term basis is likely to incur the ultimate loss of funds.

What is useful in PPRA, however, are the very detailed guidelines provided to schools for drafting "privacy" policies.⁷⁶ Among the provisions that such policies must include are protections for privacy in the administration of research surveys that ask questions about personal behavior and beliefs;⁷⁷ policies for physical examinations;⁷⁸ and procedures for the collection, disclosure, or use of personal student information for marketing purposes and the prohibition of further tertiary disclosure.⁷⁹

In creating the outlines for these policies, "personal information" over which PPRA seeks to create local policies is significantly more confined than that set out as directory information in FERPA. PPRA's "personal information" includes only student and parent names, home address, telephone number, and social security number.⁸⁰ However, the local policy need not include, and thus there seems to be no parental consent necessary for, the disclosure of this information on a much broader scope than allowed by FERPA, to entities whose exclusive purpose is the development and provision of educational products, such as college or military recruitment; access to low-cost literacy programs; curriculum and instructional materials; testing and other assessment programs designed to procure cognitive, evaluative, achievement, and aptitude information about students; student fundraising organizations; and student recognition programs.⁸¹

Attendant to these exceptions is the lack of protection for further disclosure and sale of such lists—including social security numbers—by these third parties. PPRA disclosure also implicitly allows the sale of this information inasmuch as, in an annual notice, a school must

75. 20 U.S.C. § 1232h(e).

76. *Id.* § 1232h(c).

77. *Id.* § 1232h(c)(1)(B) (including such behavior and beliefs as political affiliations, psychological problems, sexuality, criminal or demeaning behavior, criticisms of family members, legally recognized privileges, religious affiliations, and income); see also 34 C.F.R. § 98.4 (2005). One social commentator spoke of these "intrusions" not as family privacy issues but as individual privacy issues: "[T]he public schools are dealing with an essentially captive audience. The law requires that parents send their children to schools Thus, we are talking about the use of devices that probe into the private world of the student by government-operated institutions that require compulsory attendance." VANCE PACKARD, *THE NAKED SOCIETY* 137 (1964); see also *PRIVACY REPORT*, *supra* note 69, at 420.

78. 20 U.S.C. § 1232h(c)(1)(D).

79. *Id.* § 1232h(c)(1)(E). Other nonprivacy, parental "rights" provisions that must be in the annual PPRA notice include parental right to inspect research materials sought to be administered by the school to students; parental right to inspect instructional materials; and parental right to inspect the instruments collecting the aforementioned personal information. *Id.* § 1232h(c)(1)(A), (C), (F).

80. *Id.* § 1232h(c)(6)(E).

81. *Id.* § 1232h(c)(4)(A).

advise parents of any activity that involves “the collection, disclosure, or use of personal information collected from students for the purpose of marketing or for selling that information (or otherwise providing that information to others for that purpose).”⁸²

C. Individuals with Disabilities Education Act

The Individuals with Disabilities Education Act (“IDEA”)⁸³ authorizes funding to public schools⁸⁴ to provide a free appropriate public education for children with disabilities.⁸⁵ Among IDEA’s statutory charges to the DOE for this mission was the promulgation of regulations that would be in accord with FERPA to protect confidential and personally identifiable information.⁸⁶ Such DOE regulations then serve as drafting guidelines for state educational agencies to promulgate their own regulatory regimes over the local educational agencies, which ultimately use the funding and provide the special education services.⁸⁷

Special education students may well have greater privacy rights than general education students because FERPA’s charges have been incorporated by reference into IDEA, which is enforceable by a private right of action.⁸⁸ Although IDEA may suffer the ultimate fate of

82. *Id.* § 1232h(c)(2)(C)(i).

83. 20 U.S.C. §§ 1400–1482 (2000 & Supp. I 2001 & Supp. II 2002).

84. IDEA was recently reauthorized in November 2004, *see* Individuals with Disabilities Education Improvement Act of 2004, H.R. 1350, 108th Cong. (2004), and became effective July 1, 2005. There are no significant changes in the confidentiality provisions of IDEA. *See* 34 C.F.R. pt. 300 (2005).

85. Specifically, states desiring these federal funds must ensure that students with disabilities receive a “free appropriate public education that emphasizes special education and related services designed to meet their unique needs and prepare them for employment and independent living” 20 U.S.C. § 1400(d); *see also id.* § 1415(a).

86. *See id.* § 1417(c) (“The Secretary shall take appropriate action, in accordance with the provisions of section 1232g of this title, to assure the protection of the confidentiality of any personally identifiable data, information, and records collected or maintained by the Secretary and by State and local educational agencies”); Daggett, *Buckley I*, *supra* note 12, at 644. As of July 1, 2005, 20 U.S.C. § 1417(c) was changed to read: “The Secretary shall take appropriate action, in accordance with section 1232g of this title, to ensure the protection of the confidentiality of any personally identifiable data, information, and records collected or maintained by the Secretary and by State *educational agencies* and local educational agencies pursuant to this subchapter.” H.R. 1350, § 617(c) (emphasis added).

87. *See, e.g.*, 34 C.F.R. § 300.127 (“The State must have on file in detail the policies and procedures that the State has undertaken to ensure protection of the confidentiality of any personally identifiable information, collected, used, or maintained”).

88. Incorporating one statute into a later enactment, by reference, is a common practice and thereby brings the incorporated statute into the referencing statute. *See, e.g.*, *Pan. R.R. Co. v. Johnson*, 264 U.S. 375, 395–97 (1924); *see also* U.S. Dep’t of

FERPA—that as a spending clause enactment, it harbors no such enforceable rights—the Supreme Court has not yet addressed that question as it did in *Gonzaga University*. For the time being, IDEA is alternatively interpreted to create a private right of action⁸⁹ and to be enforceable under § 1983 by lower federal courts, at least with regard to the due process provisions of the IDEA.⁹⁰ Therefore, insofar as FERPA is incorporated by reference into IDEA, special education students and their parents may indeed have greater privacy rights than general education students. That does not necessarily change the fact that FERPA has serious deficiencies in the manner in which it has been crafted, drafted, and interpreted. However, engrafting IDEA's due process procedures on to FERPA's confidentiality provisions

Energy v. Ohio, 503 U.S. 607, 617 (1992). Such adoption by reference makes the earlier, incorporated statute a part of the later, referencing statute as if it had been set forth in toto. *See, e.g.*, *Engel v. Davenport*, 271 U.S. 33, 38 (1926); *Artistic Entm't, Inc. v. City of Warner Robins*, 331 F.3d 1196, 1206–07 (11th Cir. 2003), *reh'g denied*, 87 F. App'x 716 (2003), *cert. denied*, 541 U.S. 988 (2004). Typically, the incorporated statute's meaning is construed at the time of incorporation. *See, e.g.*, *United States v. One Big Six Wheel*, 987 F. Supp. 169, 177 (E.D.N.Y. 1997), *aff'd*, 166 F.3d 498, 502 (2d Cir. 1999). The reference can be specific—by citing the title of the statute, for example—by which any later changes to the incorporated statute do not affect the referencing statute. Or the reference can be general—by citing “all federal laws,” for example—by which later changes *do* affect the referencing statute. *See, e.g.*, *In re Black*, 225 B.R. 610, 621 (M.D. La. Bankr. 1998); *see also Herrmann v. Cencom Cable Assocs.*, 978 F.2d 978, 983 (7th Cir. 1992). With regard to construing the incorporated statute, the purpose and effect of the referencing statute prevail. *EEOC v. N. Gibson Sch. Corp.*, 266 F.3d 607, 621 (7th Cir. 2001) (interpreting an incorporated portion of the Fair Labor Standards Act in congruence with the purpose of the referencing Age Discrimination in Employment Act).

89. 20 U.S.C. § 1415(b)(6); *Beth V. ex rel. Yvonne V. v. Carroll*, 87 F.3d 80, 85–86 (3d Cir. 1996); *see also Asbury Park Bd. of Educ. v. Hope Acad. Charter Sch.*, 278 F. Supp. 2d 417, 421 (D.N.J. 2003). *But see Va. Office of Prot. & Advocacy v. Va. Dep't of Educ.*, 262 F. Supp. 2d 648, 658–59 (E.D. Va. 2003) (acknowledging that IDEA provides a private cause of action for noncompliance with its due process procedures but not for all the general provisions outlined in 20 U.S.C. § 1415). *See generally* Bradford C. Mank, *Suing Under § 1983: The Future After Gonzaga University v. Doe*, 39 Hous. L. Rev. 1417, 1475–79 (2003) (outlining the federal circuit courts' decisions with regard to enforcement under IDEA).
90. *E.g.*, *Quackenbush v. Johnson City Sch. Dist.*, 716 F.2d 141, 148 (2d Cir. 1983); *B.H. v. Southington Bd. of Educ.*, 273 F. Supp. 2d 194, 203–04 (D. Conn. 2003), *modified on other grounds*, No. Civ.A. 302CV252SRU, 2004 WL 51001 (D. Conn. Jan. 7, 2004); *Goleta Union Elementary Sch. Dist. v. Ordway*, 166 F. Supp. 2d 1287, 1292 (C.D. Cal. 2001). *Contra Sellers ex rel. Sellers v. Sch. Bd. of Manassas, Va.*, 141 F.3d 524, 529–30 (4th Cir. 1998); *Monticello Sch. Dist. No. 25 v. George L. ex rel. Brock L.*, 102 F.3d 895, 903–04 (7th Cir. 1996); *see also* 34 C.F.R. § 300.512 (“Any party aggrieved by the findings and decisions made under [certain due process provisions] has the right to bring a civil action . . . in any State court of competent jurisdiction or in a district court of the United States without regard to the amount in controversy.”).

makes breaches of those provisions subject to private suit under IDEA and not just a slap on the wrist by the DOE.⁹¹

Furthermore, the IDEA regulations⁹² pertaining to student records and the due procedures surrounding those records are more favorable to parents and students than those implementing FERPA.⁹³ Those regulations protect the same records protected by FERPA⁹⁴ and set out notice requirements for parents (particularly as to the destruction of any records);⁹⁵ parental access rights in general with regard to log of access, locations, and types of records;⁹⁶ parental access rights in particular with regard to parent participation in special education meetings; and record amendment procedures.⁹⁷ And parents of special education students have particular enforcement rights under the comprehensive administrative procedures provided in the IDEA regulations.⁹⁸

IDEA also has some features distinct from FERPA. One positive distinction is that schools may only make nonconsensual disclosures of or otherwise provide access⁹⁹ to personally identifiable information¹⁰⁰ for the purpose of serving the child under the IDEA.¹⁰¹ A second posi-

-
91. *P.N. v. Greco*, 282 F. Supp. 2d 221, 245 (D.N.J. 2003). In *P.N.*, a public school district and its special education director were unsuccessfully sued for their disclosure of personally identifiable information under FERPA. *Id.* at 244–45. However, the claim was successful under IDEA via § 1983. *Id.* at 245–46; see also *Taylor v. Vt. Dept. of Educ.*, 313 F.3d 768, 786 (2d Cir. 2002) (holding that a parent has a right of access to educational records under the IDEA); *Sean R. ex rel. Dwight R. v. Bd. of Educ. of Woodbridge*, 794 F. Supp. 467, 469 (D. Conn. 1992). In *Sean R.*, a special education student stated a derivative IDEA cause of action under § 1983 for a school's disclosure of confidential information by arguing that a parent has "expectations" of privacy by virtue of IDEA's comprehensive regulations. *Id.* at 468–69.
 92. These IDEA regulations are obviously subject to numbering changes since the Act's reauthorization and the DOE's task of updating the regulations to conform to the changes.
 93. Compare 34 C.F.R. §§ 300.560–.577, with 34 C.F.R. pt. 99; see also Daggett, *Buckley I*, *supra* note 12, at 644 & n.208.
 94. 34 C.F.R. § 300.560(b).
 95. *Id.* §§ 300.561, .573.
 96. *Id.* § 300.562.
 97. *Id.* § 300.567. See generally Daggett, *Buckley I*, *supra* note 12, at 644–48 (discussing the provisions of IDEA).
 98. See Daggett, *Buckley I*, *supra* note 12, at 647–48.
 99. Each educational agency must keep a record of the employees who have authorized access to IDEA student records. 34 C.F.R. § 300.572(d).
 100. *Id.* § 300.500(b)(3) ("Personally identifiable means that information includes: (i) The name of the child, the child's parent or other family member; (ii) The address of the child; (iii) A personal identifier, such as the child's social security number or student number; or (iv) A list of personal characteristics or other information that would make it possible to identify the child with reasonable certainty.").
 101. *Id.* § 300.571. Nonconsensual disclosures may also be made as otherwise constrained by FERPA. *Id.* § 300.571(b). Any use of the information by the DOE itself is subject to the Privacy Act of 1974. *Id.* § 300.577.

tive distinction is the explicit provision for the child to wield rights over his own records: "The [state educational agency] shall provide policies and procedures regarding the extent to which children are afforded rights of privacy similar to those afforded to parents, taking into consideration the age of the child and type or severity of disability"¹⁰² with rights concomitant to FERPA's. In any event, the rights transfer to a special education student when he reaches eighteen years of age.¹⁰³ A third positive distinction requires that each educational agency designate one individual who is particularly charged with maintaining the confidentiality of personally identifiable information.¹⁰⁴

IDEA also has one singularly negative provision concerning education informational privacy, and that is the provision that an educational "agency reporting a crime committed by a child with a disability shall ensure that copies of the special education and disciplinary records of the child are transmitted for consideration by the appropriate authorities to whom it reports the crimes."¹⁰⁵ This mandate directly contradicts the restraints in FERPA.¹⁰⁶ There is no rational explanation why special education students should be treated differently than general education students in this regard. In contrast, the IDEA regulation concerning procedural implementation of this provision incorporates FERPA as a limiting factor in the transmission of student records merely on request and may well limit this otherwise unrestricted power to hand over personal records to law enforcement officials to instances when properly entered court orders and subpoenas are presented.¹⁰⁷ Otherwise, by itself and without FERPA's limits, this unique IDEA provision is an unconstitutional violation under the Fourth Amendment and perhaps the Fifth as well.

The unique mission of IDEA also militated special concern for the confidentiality of medical information in student files not otherwise

102. *Id.* § 300.574(a).

103. Compare *id.* § 300.574 (providing that records rights transfer at age eighteen), with 20 U.S.C. § 1415(m) (2000) (providing that parental rights may transfer at the state age of majority).

104. 34 C.F.R. § 300.572; Daggett, *Buckley I*, *supra* note 12, at 646.

105. 20 U.S.C. § 1415(k)(6)(B) (originally enacted as 20 U.S.C. § 1415(k)(9)(B)); 34 C.F.R. § 300.529(b); see also Dixie Snow Huefner & Lynn M. Daggett, *FERPA Update: Balancing Access and Privacy of Student Records*, 152 W. EDUC. L. REP. 469, 488 (2001).

106. Thomas A. Mayes & Perry A. Zirkel, *Disclosure of Special Education Students' Records: Do the 1999 IDEA Regulations Mandate that Schools Comply with FERPA?*, 8 J.L. & POL'Y 455, 460-61 (2000).

107. 34 C.F.R. § 300.529(b)(2); see Mayes & Zirkel, *supra* note 106, at 466-71. But see *Commonwealth v. Nathaniel N.*, 764 N.E.2d 883, 887-88 (Mass. App. Ct. 2002). In *Nathaniel N.*, a special education student unsuccessfully sued the school district for an IDEA violation in *failing* to turn his school records over to the police. *Id.*

addressed in FERPA. Any kind of mental, physical, or psychological disability that warrants placement in special education is necessarily going to require a plethora of documentation, inevitably including private medical information. That information is placed in students' education records, for health and safety as well as pedagogical reasons. Under IDEA, access to those records is very limited—on a “need-to-know” basis—and confidentiality is maintained so tightly that medical information should be difficult to access.¹⁰⁸ Although IDEA has no comparable protection over separately maintained medical records as exists for employees under the Americans with Disabilities Act (“ADA”)¹⁰⁹ itself, as a practical matter, any local educational agency worth its salt will maintain those records in a location apart from the general education records of the rest of the student population.¹¹⁰

D. Student Medical Information

One point of similarity between special education students and general education students is the concern about medical information regardless of disability. Educational agencies must be familiar with four principle areas of privacy protection with regard to students' medical information: (i) the general constitutional protections; (ii) Health Insurance Portability and Accountability Act of 1996 (“HIPAA”);¹¹¹ (iii) the privilege of school nursing files; and (iv) substance abuse documentation.

108. *But see* Valentino C. v. Sch. Dist. of Philadelphia, No. Civ.A. 01-2097, 2003 WL 177210, at *11 (E.D. Pa. Jan. 23, 2003). In *Valentino C.*, a special education student sued the school district for *failing* to forward his medical records to police pursuant to the IDEA when he was arrested for a violent classroom incident. *Id.*

109. 42 U.S.C. § 12112(d)(3)(B), (d)(4)(C) (2000). “Information obtained . . . regarding the medical condition or history of [any employee] shall be collected and maintained on separate forms and in separate medical files and be treated as a confidential medical record” 29 C.F.R. § 1630.14(b)(1) (2005); *see also* Rehabilitation Act, 29 U.S.C. § 794(d) (Supp. II 2002); *Stokes v. Barnhart*, 257 F. Supp. 2d 288, 294 (D. Me. 2003) (finding that ADA standards apply to Rehabilitation Act claims). *But see Stokes*, 257 F. Supp. 2d at 294–95 (holding that the Rehabilitation Act did not apply to a claim of privacy violation for disclosure of medical records outside the employment arena). *See generally* Doe v. U.S. Postal Serv., 317 F.3d 339 (D.C. Cir. 2003) (discussing the interplay between the Rehabilitation Act, the ADA, and the Privacy Act of 1974).

110. However, Atlanta schools and those in surrounding counties have been routinely providing access to special education records to the Centers for Disease Control and Prevention without student or parental consent. Mark Walsh, *CDC Access to Students' Health Records Raises Questions of Privacy*, EDUC. WEEK, April 30, 2003, at 32, available at 2003 WLNR 6596211.

111. Pub. L. No. 104-191, 110 Stat 1936 (1996).

1. *Medical Records, Generally*

The medical files of any child with a serious medical condition—whether disabling or not—may be at the fingertips of school personnel. Even if not for use under IDEA, such records are maintained for health and safety purposes. Similar concerns surround those records generated by and kept by school psychologists or other therapists employed by the school,¹¹² providing services to both IDEA-protected children and others. The privacy concern is disclosure of and access to that medical information.¹¹³

The threshold protection for these records is from any dissemination—either by access or disclosure—of private information as addressed in *Whalen v. Roe*. Medical privacy is a constitutional right that requires a strong state interest in government collection and disclosure.¹¹⁴ Disclosure of such information “unquestionably offends those ‘basic and fundamental rights’ which we consider so ‘deeply rooted in our society’ as to directly bear on our privacy rights.”¹¹⁵ For public schoolchildren, this constitutional right derives from the Fourteenth Amendment.¹¹⁶ This constitutional right does not prohibit

112. Mental health records of students are entitled to the same policy considerations in terms of confidentiality as juvenile records because of the stigma that may attach. *W. Va. Dept. of Health & Human Res. v. Clark*, 543 S.E.2d 659, 662 (W. Va. 2000).

113. Deliberate government collection of such data is, of course, limited by *Whalen v. Roe*. See *supra* notes 2–5. In addition, the state must have a compelling interest in the collection of such records. Compare *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 580–81 (3d Cir. 1980) (holding that before medical records of private-sector employer can be turned over pursuant to federal subpoena duces tecum, each employee must be notified and given an opportunity to object), with *Clark*, 543 S.E.2d at 663 (holding that the state department of health and human resources must show probable cause before reviewing school and medical records of private schools’ students). But see *United States v. District of Columbia*, 44 F. Supp. 2d 53, 61–62 (D.D.C. 1999) (holding that the government’s interest in the collection of mental health records of defendants hospitalized after being found not guilty by reason of insanity outweighed the defendant–patients’ privacy interests because the patients had made their mental conditions a matter of public record and because the government had financial responsibility for their care).

114. See, e.g., *Denius v. Dunlap*, 209 F.3d 944, 956 (7th Cir. 2000).

115. *Mann v. Univ. of Cincinnati*, 152 F.R.D. 119, 126 (S.D. Ohio 1993) (holding that the university violated the student’s constitutional rights when it disclosed her medical records before the date set out in the subpoena and without informing the student), *aff’d*, 114 F.3d 1188 (6th Cir. 1997).

116. See, e.g., *Gruenke v. Seip*, 225 F.3d 290, 302–03 (3d Cir. 2000) (holding that a high school swim coach violated a team member’s constitutional privacy rights when he required her to take a pregnancy test). But see *Hedges v. Musco*, 204 F.3d 109, 121 (3d Cir. 2000) (holding that a school nurse did not violate constitutional privacy rights when she inadvertently revealed a student’s drug-testing results); *Duda v. Bd. of Educ. of Franklin Park Pub. Sch. Dist. No. 84*, 133 F.3d 1054, 1062 (7th Cir. 1998) (determining that *Whalen v. Roe* does not apply to public employees’ distribution of a personal diary of a mentally disabled co-employee); *Demers v. Leominster Sch. Dep’t*, 263 F. Supp. 2d 195, 203–04 (D. Mass.

school officials from having access to the information: health and safety issues would demand such access.¹¹⁷ However, such access to these records should be limited, and the records themselves should be in a secure location, similar to the privacy provided to employee medical information under the ADA¹¹⁸ and to special education records under IDEA.

2. HIPAA

In Spring 2001, health data privacy protections were mandated by HIPAA.¹¹⁹ The impetus for these privacy protections arose from the personal nature of health information and the proliferation of electronic databases to collect and store that information. This type of "protected health information" includes intimate details of both physical and mental health—information traditionally protected by the doctor-patient privilege—and could be the source of stigmatization and discrimination if disclosed.¹²⁰

HIPAA regulates electronic communications between health-care providers and health insurers to protect individually identifiable health information. For determining whether they must conform to HIPAA, schools must be either a "health care provider"¹²¹ or any person who, "in the normal course of business, furnishes, bills, or is paid for 'health care'" and who transmits health information electronically.¹²² A protected HIPAA transaction is an exchange of information to carry out financial and administrative activities concerning

2003) (holding that requiring a student to undergo a psychiatric examination in the interest of school safety would not have been a constitutional privacy violation).

117. See, e.g., *Doe v. Delie*, 257 F.3d 309, 317 (3d Cir. 2001) (holding that a prison inmate has a constitutional right to medical privacy that can only be "curtailed by a policy or regulation that is shown to be reasonably related to legitimate penological interests").
118. 29 C.F.R. § 1630.14 (2005). Title II of the ADA prohibits discrimination in public services. 42 U.S.C. § 12132 (2000). It applies to schools. See, e.g., *Weixel v. Bd. of Educ.*, 287 F.3d 138 (2d Cir. 2002).
119. 42 U.S.C. § 1320d to d-8 (2000 & Supp. II 2002); see also Pub. L. No. 104-191, 110 Stat. 1936 (1996).
120. Judith Wagner DeCew, *The Priority of Privacy for Medical Information*, in *THE RIGHT TO PRIVACY* 213, 213–14 (Ellen Frankel Paul et al. eds., 2000); Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 489–92 (1995) (outlining a health information system before the codification of HIPAA).
121. 45 C.F.R. pt. 164 (2005); JILL MOORE & AIMEE WALL, *APPLICABILITY OF HIPAA TO HEALTH INFORMATION IN SCHOOLS* 1–2 (2003), <http://www.medicalprivacy.unc.edu/pdfs/schools.pdf>; Michael Levin et al., *What to Do When the HIPAA Beast Is at Your Door*, INQUIRY & ANALYSIS, Jan. 2003, at 1, 1–2, available at <http://www.nsba.org/site/docs/10900/10850.pdf>.
122. MOORE & WALL, *supra* note 121, at 2; Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 643 (2002).

health care.¹²³ The protected product, "individually identifiable health information," is

information that is created or received by a healthcare provider . . . that relates to the physical or mental health of an individual, as well as the provision of healthcare to an individual or payment for the provision of healthcare to an individual, and that identifies the individual or could be used to identify the individual.¹²⁴

Based on the circuitous language of HIPAA, a local educational agency would benefit from some expert advice on determining its status under the statute.

What is equally important to note, however, is that "education records" covered by FERPA originally had been excluded from the HIPAA privacy rule's classification for "protected health information."¹²⁵ However, the definition of "protected health information" was removed from the HIPAA privacy rule.¹²⁶ Apparently, the DOE assumes that FERPA-related records are excluded from HIPAA's protection because the exclusion still exists in regulations for the Social Security Act.¹²⁷ Thus, the protection of and access to FERPA-related health records under HIPAA remain a mystery.

Regardless, HIPAA's protected health information would still likely include any documentation, such as personal notes or information, held solely by an individual school psychologist or physical therapist. Those records are typically considered outside the scope of FERPA-protected education records and would therefore not be affected one way or the other by HIPAA coverage of FERPA records.¹²⁸ Except for a few limited circumstances, the patient must consent to the disclosure and use of this personal health information under HIPAA. One of those limited circumstances is when parents of an unemancipated minor may be entitled to disclosure of or access to the records as the child's personal representatives unless prohibited by state law.¹²⁹

123. MOORE & WALL, *supra* note 121, at 2.

124. Winn, *supra* note 122, at 644; see 42 U.S.C. § 1320d(6); 45 C.F.R. § 160.103.

125. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182, 53,266-67 (Aug. 14, 2002) (codified at 45 C.F.R. § 164.501); see, e.g., Stephen J. McDonald & Barbara L. Shiels, *FERPA: New Issues for Our Old Friend*, in *THE FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT: A LEGAL COMPENDIUM* 537, 548-49 (Nat'l Assoc. of Coll. & Univ. Att'ys, Stephen J. McDonald ed., 2d ed. 2002) [hereinafter *LEGAL COMPENDIUM*] (on file with the NEBRASKA LAW REVIEW); MOORE & WALL, *supra* note 121, at 2.

126. Health Insurance Reform: Security Standards, 68 Fed. Reg. 8,334, 8,380 (Feb. 20, 2003).

127. See 45 C.F.R. § 160.103; Family Educational Rights and Privacy Act, 69 Fed. Reg. 21,670, 21,672 (Apr. 21, 2004).

128. Levin et al., *supra* note 121, at 4.

129. 45 C.F.R. § 164.502(g); Lawrence O. Gostin et al., *The Nationalization of Health Information Privacy Protections*, 37 TORT & INS. L.J. 1113, 1115-16, 1135 (2002). Other exemptions include court-ordered disclosure, matters of public health, and

There are also two particular functions with which public schools must be concerned under HIPAA: student health clinics and school nurses. HIPAA regulates either function if it transmits information electronically. Student health clinics would most clearly come within the protections of HIPAA because of the type of information they obtain and because the information is not likely to fall within the FERPA exceptions.¹³⁰ The situation is a bit more complicated with regard to a school nurse. If the nurse transmits electronic health information in a HIPAA transaction, she is covered. If she does not transmit electronically, then it depends upon whether her employer—the local school—*ever* transmits electronic health information. If so, the nurse is also within HIPAA. However, if the employer does transmit electronically but takes action to exclude the nursing program from HIPAA coverage as a “hybrid” entity, the school nurse is not covered.¹³¹ The whole rigamarole is pretty convoluted, but the gist of HIPAA is that schools may have to comply with HIPAA’s use and disclosure requirements, notice and access requirements, and administrative procedural requirements.¹³²

The HIPAA privacy rule is a short list of permitted and required disclosures of protected health information; all other disclosures are prohibited.¹³³ *Required* disclosures are made to the affected individual under a right of access and to the Department of Health and Human Services to check HIPAA compliance.¹³⁴ *Permitted* disclosures are made to the individual; to carry out health care treatment and its payment in accordance with patient authorization or advance notice to the patient as agreed; and for certain health and safety issues.¹³⁵ An educational agency that is required to follow HIPAA and its privacy rules¹³⁶ must be prepared to implement procedures for statutorily mandated patient access to and power to amend her health records; procedures to maintain the privacy of health records and to notify patients of such procedures; and procedures for confidential

health research. *Id.* at 1115. However, the DOE seems confused about parental access to children’s medical information and state law prohibitions to disclosure. See Letter from LeRoy S. Rooker, Director, Family Policy Compliance Office, to Robert H. Henry, Attorney, School and College Legal Services of California (Mar. 14, 2005), available at <http://www.ed.gov/policy/gen/guid/fpco/ferpa/library/ca031405.html>.

130. MOORE & WALL, *supra* note 121, at 4; see also McDonald & Shiels, *supra* note 125, at 549 (discussing the potential application of HIPAA to campus health and counseling clinics at postsecondary institutions).

131. MOORE & WALL, *supra* note 121, at 4–7; Levin et al., *supra* note 121, at 1–2.

132. See generally MOORE & WALL, *supra* note 121.

133. 45 C.F.R. § 164.502(a). See generally MOORE & WALL, *supra* note 121, at 7–11.

134. 45 C.F.R. § 164.502(a)(2).

135. *Id.* § 164.502(a)(1).

136. *Id.* pt. 164.

communications and accounting for actual disclosures.¹³⁷ Among those duties, the educational agency must designate a privacy officer responsible for implementing the various privacy, administrative, technical, and physical standards and safeguards necessary to comply with HIPAA and its regulations.¹³⁸ Because of the intricacies involved in HIPAA compliance, an educational agency should make certain this officer is adequately trained and that all notices and procedures follow a national standard rather than a local standard. Although the appropriate notices of individual rights under HIPAA could be disseminated with other notices, the formulation and implementation of these complex matters is not lightly left to the local educational agencies themselves.

3. *School Nurses*

HIPAA does not cover all the privacy issues inherent in school nursing duties. For nurses to comply with appropriate nursing standards, they have to keep "process documentation." And although that documentation need not necessarily become part of a state-required school health record—for immunizations, for instance—nor otherwise entered in the student's cumulative record, there is the potential that such systematic documentation could be considered an educational record under FERPA, subject to the same problematic disclosure standards and parental access.

School nurses often keep systematic process documentation through daily logs of student visits in order to provide a plan of appropriate nursing care to the students. Not all of this information is transferred to the school health record forms, and some of the information remaining in these logs is confidential. The logs must be maintained for the nursing process but are separate from the formally maintained records. However, these logs might be accessible under FERPA because they probably are not the "personal notes" that might otherwise be exempt from disclosure as education records.¹³⁹ Thus, a school nurse runs into a real conflict if approached for health advice, particularly from a mature minor, if she documents that meeting in accordance with nursing standards. Parents may be able to access that documentation under FERPA.¹⁴⁰

137. See Gostin et al., *supra* note 129, at 1115.

138. MOORE & WALL, *supra* note 121, at 7–11; Levin et al., *supra* note 121, at 2.

139. See Mary H.B. Gelfman & Nadine C. Schwab, *School Health Services and Educational Records: Conflicts in the Law*, 64 W. EDUC. L. REP. 319, 323–25 (1991); see also NAT'L SCH. BDS. ASS'N, GUIDANCE FOR SCHOOL DISTRICTS ON STUDENT EDUCATION RECORDS, DIRECTORY INFORMATION, HEALTH INFORMATION AND OTHER PRIVACY PROVISIONS 4 (2004), <http://www.nsba.org/site/docs/32500/32420.pdf>.

140. See Daggett, *Buckley I*, *supra* note 12, at 649.

4. *Drug and Alcohol Abuse Records*

Any student who is a patient in a federally assisted drug or alcohol abuse program has a nearly absolute right of confidentiality in those records under the Public Health Services Act.¹⁴¹ The confidentiality of the information resides in the patient, and disclosure usually requires written consent. If state law confers the legal capacity upon minors to obtain substance abuse treatment, then only the minor patient may consent to disclosure; however, if state law requires the consent of a parent or guardian for such treatment, then both the minor and parent must sign the consent¹⁴² unless the minor "lacks the capacity for rational choice."¹⁴³ Disclosure without such consent is limited to medical emergencies, certain research projects, audit and evaluation procedures,¹⁴⁴ and certain court orders.¹⁴⁵ The disclosure of these records is even circumscribed in criminal proceedings in the absence of "good cause" for the information in investigating or charging a patient.¹⁴⁶

A school may be affected by the Public Health Services Act if it is an "entity . . . who holds itself out as providing, and provides, alcohol or drug abuse diagnosis, treatment or referral for treatment"¹⁴⁷ that receives federal assistance. Such "treatment" certainly includes substance abuse education and prevention and likely includes any counseling undertaken at an educational agency.¹⁴⁸ Federal assistance need not be directly related to the provision of drug or alcohol treatment to require a governmental agency to comply with the statute's confidentiality provisions.¹⁴⁹ Because these written records must be

141. 42 U.S.C. § 290dd-2 (2000) ("Records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any program or activity relating to substance abuse education, prevention, training, treatment, rehabilitation, or research, which is conducted, regulated, or directly or indirectly assisted by any department or agency of the United States shall . . . be confidential . . ."); *see also* 42 C.F.R. § 2.3 (2005). Because this statutory provision is essentially a criminal prohibition, it creates no individual right to enforcement and is not otherwise enforceable under § 1983. *See, e.g., Doe v. Broderick*, 225 F.3d 440, 447 (4th Cir. 2000).

142. 42 C.F.R. § 2.14. There is also a restriction on the disclosure of an *application* for treatment to parents, even in states where parental consent is required for the treatment itself.

143. *Id.* § 2.14(d).

144. *Id.* pt. 2, subpt. D.

145. *Id.* pt. 2, subpt. E.

146. 42 U.S.C. § 290dd-2(b)(c).

147. 42 C.F.R. § 2.11 (defining "program" for the purposes of the Public Health Services Act).

148. *See also* FORUM GUIDE, *supra* note 8, at 20 (suggesting that counseling for children of substance abusers may be sufficient to trigger the protections of the Public Health Services Act).

149. 42 C.F.R. § 2.12(b)(3).

locked up and secure,¹⁵⁰ they should be separated from the usual education records. Depending upon state law treatment of minors, parental access to the records may be limited so segregating those records is a wise idea.¹⁵¹

This statute also raises a dilemma for the increasingly common drug-testing programs in schools—programs designed to control drug use by agencies that receive federal funds. The statute's restrictions on disclosure do not apply to law enforcement personnel for crimes on the premises.¹⁵² However, if, for example, a student tests positive for Tetrahydrocannabinol (commonly called THC)¹⁵³ during a school-implemented drug test after having smoked marijuana two weeks before, the student has not really committed a "crime on the premises" under the statute. Furthermore, because the statute's confidentiality provision is not confined to written records,¹⁵⁴ a school that takes disciplinary action as a result of a drug test—such as prohibiting the student from taking part in extracurricular activities—might be "publicizing" this information in violation of the statute.¹⁵⁵

E. Children's Online Privacy Protection Act¹⁵⁶

Although intimately concerned with children's privacy, the Children's Online Privacy Protection Act ("COPPA") has limited application to schools.¹⁵⁷ COPPA is basically a fair information practices regime that protects children in their private-sector, on-line activities

150. *Id.* § 2.16.

151. The DOE's suggestion that a minor student must waive his right of confidentiality from parental access as a condition for receiving these services is likely a violation of a mature minor's right to decisional privacy if required by the state and unlawfully elicited without the benefit of counsel. *See* FORUM GUIDE, *supra* note 8, at 20. *But see* Bellotti v. Baird, 443 U.S. 622 (1979) (holding a Massachusetts abortion law unconstitutional because it made a minor child's ability to obtain an abortion absolutely conditional on the consent of both parents).

152. 42 C.F.R. § 2.12(c)(5).

153. THC, the psychoactive ingredient in marijuana, can remain in the system of a frequent user of marijuana up to six weeks after consuming the drug. *See* Home Drug Testing Kit, How Long Do Drugs Stay in a Person's System?, http://www.homedrugtestingkit.com/drug_info.html#howlong (last visited May 15, 2006).

154. 42 C.F.R. § 2.11 (defining "records" for the purposes of the Public Health Services Act).

155. *See, e.g.,* Jeanette A. v. Condon, 728 F. Supp. 204, 206 (S.D.N.Y. 1989) (holding that a police officer could not be discharged on the basis of a urinalysis test conducted after completing the department's federally assisted substance abuse program when she had not consented to release of the results).

156. 15 U.S.C. §§ 6501–6506 (2000).

157. *Id.* As a response to the absence of the internet industry's self-regulation, the key components of COPPA are (i) notice; (ii) parental consent; (iii) parental review; (iv) limits on the use of online games and prizes; and (v) security. Laurel Jamtgaard, *Big Bird Meets Big Brother: A Look at the Children's Online Privacy Protection Act*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 385, 386, 388 (2000).

and governs website operators' collection, maintenance, and use of personal information from children under the age of thirteen.¹⁵⁸ Congress enacted COPPA to address the collection and use of online personal information from children, especially information with commercial value.

Collection concerns are twofold. First, *active* collection of personal information is direct solicitation of personal information—name, address, e-mail address, age, gender, and telephone number. Second, *surreptitious* collection involves passive data collection provided to the website operator inherent in the use of the medium itself through the use of “cookies,” which identify such things as the user’s computer identification and the type of sites visited.¹⁵⁹ COPPA was intended to protect children from both online and physical contact and requires the collection of identifiable information only with “verifiable” parental consent. Thus, it protects the collection of names, home addresses, e-mail addresses, telephone numbers, and the like.¹⁶⁰

-
158. See Allen, *supra* note 51, at 758; Nancy L. Savitt, *A Synopsis of the Children's Online Privacy Protection Act*, 16 ST. JOHN'S J. LEGAL COMMENT. 631, 631 (2002); Danielle J. Garber, Note, *COPPA: Protecting Children's Personal Information on the Internet*, 10 J.L. & POL'Y 129, 132 (2001).
159. Garber, *supra* note 158, at 134–38; cf. Jennifer C. Wasson, Recent Developments, *FERPA in the Age of Computer Logging: School Discretion at the Cost of Student Privacy?*, 81 N.C. L. REV. 1348, 1362–64 (2003) (positing that FERPA should provide privacy protections over “logging,” or the collection of data by a systems administrator).
160. 15 U.S.C. § 6501(8). COPPA has been criticized for limiting its scope to preteens. See Allen, *supra* note 51, at 759–60. Teenagers are a huge consumer population, and excepting the use of their personally identifiable information, particularly as a marketing tool, seems an extraordinary lapse by Congress. Teen markets are the sole reason for Chris Whittle to place “Channel One,” see ChannelOne.com, About Channel One, <http://www.channelone.com/common/about> (last visited May 15, 2006), and its advertising in high school classrooms throughout the country. On the other hand, because COPPA requires parental consent before a preteen can voluntarily disclose personal information, it has also been criticized on the grounds that it abdicates preteens’ privacy interest in favor of parental control and authority. See Allen, *supra* note 51, at 773–74. So there is an inherent tension between the government’s explicit regulation of collection and disclosure of information on the one hand with the government’s implicit regulation of children’s autonomy on the other. However, safety concerns unique to children militate on the side of government protection. See Savitt, *supra* note 158, at 150–51 (noting the need for governmental regulation that requires parental consent before children can disclose personal information on the internet to “strangers”). One commentator lists five special “privacy” concerns that support the enactment of COPPA: (i) children have traditionally been protected because they are not legally capable of protecting themselves; (ii) children do not usually grasp the idea of privacy; (iii) children do not understand the use of the information being sought; (iv) online solicitations may be irresistible to children; and (v) parents are not supervising internet use. Dorothy A. Hertz, Note, *Don't Talk to Strangers: An Analysis of Government and Industry Efforts to Protect a Child's Privacy Online*, 52 FED. COMM. L.J. 429, 434 (2000).

COPPA's particular application to educational agencies occurs when they provide online access to children for which they generally need parental consent. Although not specifically provided in COPPA, neither the statute itself nor its regulations prohibit schools from acting as agents for parents in providing consent to the disclosure of information to website operators.¹⁶¹ Although some concerns exist that getting consent could be disruptive of the educational process,¹⁶² the Federal Trade Commission ("FTC") has published a guide for teachers on how to deal with COPPA in the classroom on a voluntary basis only.¹⁶³

F. Government Accountability and Education Statistics

The No Child Left Behind Act of 2001 ("NCLB"),¹⁶⁴ a comprehensive school reauthorization of the Elementary and Secondary Education Act of 1965, was intended to reform public education and affects educational privacy issues only tangentially. As mentioned above, NCLB specifically amended PPRA. Other than that, however, only its provisions addressing government accountability and transparency

Some commentators decry government involvement at all in privacy protection insofar as it affects information, preferring a more laissez-faire regulation of commercial enterprises. See, e.g., FRED H. CATE, *PRIVACY IN THE INFORMATION AGE* 103–28 (1997); LESSIG, *supra* note 61, at 160–61. However, one former state attorney general views the limited privacy protections provided by legislatures as causing all sorts of problems in his bailiwick—identity theft, telemarketing fraud, and institutional destabilization. See Mike Hatch, *The Privatization of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century*, 27 WM. MITCHELL L. REV. 1457, 1485–94 (2001). Recent disclosures that a leading credit-reporting and information-collection company, ChoicePoint, disclosed the private information of over 100,000 individuals to unauthorized parties may prompt more government controls. See Tom Zeller Jr., *Release of Consumers' Data Spurs ChoicePoint Inquiries*, N.Y. TIMES, Mar. 5, 2005, at C2, available at 2005 WLNR 3354817.

In any event, if neither self-enforcement nor the legislatures will control the sale of information, the courts will likely have to step in when the results of that sale cause harm. In a recent decision responding to a certified question, the New Hampshire Supreme Court stated that it would impose a duty on internet information brokers to exercise reasonable care in disseminating personal information so as not to subject an individual to an unreasonable risk of harm. See *Remsburg v. Docusearch, Inc.*, 816 A.2d 1001, 1007 (N.H. 2003). The underlying case concerned a woman who was killed at her workplace; the address of her workplace was provided to her killer by an information broker. *Id.* at 1006.

161. See 16 C.F.R. pt. 312 (2005); Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,903 (Nov. 3, 1999); Savitt, *supra* note 158, at 632 n.6.

162. 64 Fed. Reg. at 59,903.

163. See FED. TRADE COMM'N, *HOW TO PROTECT KIDS' PRIVACY ONLINE: A GUIDE FOR TEACHERS* (2000), <http://www.ftc.gov/bcp/online/pubs/online/teachers.pdf>. Of course, all that begs the question of the circumstances during which a child would need to give out personal information during an on-line educational activity.

164. Pub. L. No. 107-110, 115 Stat. 1425 (2002) (codified at 20 U.S.C. § 6301 (Supp. II 2002)).

have any other effect on schoolchildren's individually identifiable personal information. As NCLB insists on testing and assessment as the means and methods for school improvement and accountability in reading and mathematics, schools must necessarily allow public access to those records.¹⁶⁵ However, individual assessment statistics become part of the student's education records and are otherwise protected by the provisions of FERPA.¹⁶⁶ Also exempted from NCLB's public access is personally identifiable information about students, their academic achievement, and their parents.¹⁶⁷

Similar protections are included in the Education Sciences Reform Act of 2002.¹⁶⁸ That Act created an Institute of Education Sciences within the DOE to "provide national leadership" in the progress and condition of education in the United States.¹⁶⁹ Within the Institute are the National Center for Education Research,¹⁷⁰ the National Center for Education Statistics ("NCES"),¹⁷¹ and the National Center for Education Evaluation and Regional Assistance,¹⁷² all of which feed on statistical and other research data to justify their missions. The Institute is specifically bound by the confidentiality provisions of FERPA, PPRA, and the Privacy Act of 1974 with regard to individually identifiable information, but the remaining data is widely available to the public, especially via the Internet.¹⁷³

The USA Patriot Act, however, carved out an exception to the confidentiality protection otherwise required of the NCES.¹⁷⁴ The United States Department of Justice now has the power to collect individually identifiable information possessed by the NCES by applying in writing and averring that the information is relevant to a terrorism investiga-

165. See 20 U.S.C. § 9366(c)(1)(A) ("[P]arents and members of the public shall have access to all assessment data, questions, and complete and current assessment instruments of any assessment authorized under this section. The local educational agency shall make reasonable efforts to inform parents and members of the public about the access required under this paragraph.").

166. *Id.* § 7903.

167. *Id.* § 9366(c)(3). This provision was prompted by the Privacy Act of 1974.

168. Pub. L. No. 107-279, 116 Stat. 1940 (codified at 20 U.S.C. §§ 9501-9624).

169. 20 U.S.C. § 9511.

170. *Id.* § 9531.

171. *Id.* § 9541.

172. *Id.* § 9561.

173. *Id.* §§ 9573-9574.

174. The exception can be found at 20 U.S.C. § 9573(e). For reasons that remain somewhat of a mystery, the NCES itself suggested the exemption from confidentiality. Robert Gellman, *Education Statistics Agency Plays Loose with Privacy*, GOV'T COMPUTER NEWS, Mar. 4, 2002, http://gcn.com/21_5/tech-report/18064-1.html. Gellman suggests that NCES's cooperative attitude could open the floodgates to congressional procedures to track down student loan defaulters, deadbeat dads, and the like.

tion under circumstances similar to the seizure of educational records otherwise protected under FERPA.¹⁷⁵

G. Military Recruitment

Perhaps one of the most devilish developments in educational privacy arose from a provision found in both NCLB and the National Defense Authorization Act for Fiscal Year 2002.¹⁷⁶ Both these authorization bills require secondary schools to provide access for military recruiters to certain directory information maintained under FERPA. NCLB provides that, "[n]otwithstanding [FERPA], each local educational agency receiving assistance under this chapter shall provide, on a request made by military recruiters or an institution of higher education, access to secondary school students names, addresses, and telephone listings."¹⁷⁷ Similarly, the Defense Authorization Act's language states that "[e]ach local educational agency receiving assistance under the Elementary and Secondary Education Act of 1965 . . . shall, upon request made by military recruiters for military recruiting purposes, provide access to secondary school student names, addresses, and telephone listings, notwithstanding [FERPA]."¹⁷⁸ Only NCLB contains an exception for a private school "that maintains a [verifiable] religious objection to service in the Armed Forces."¹⁷⁹ Although not completely clear from the language of either Act's provision, student information is exempt from the military's request if the student or a parent has requested that this information not be released without prior written "parental consent."¹⁸⁰

The impetus for passage of these provisions arose when some high schools refused campus access to military recruiters because of the armed forces' policies concerning gays.¹⁸¹ The congressional enact-

175. 20 U.S.C. § 9573(e).

176. Pub. L. No. 107-107, § 544(a), 115 Stat. 1112, 1222 (codified as amended at 10 U.S.C. § 503(c) (2000 & Supp. II 2002)).

177. 20 U.S.C. § 7908.

178. 10 U.S.C. § 503(c) (Supp. II 2002).

179. 20 U.S.C. § 7908(c).

180. The NCLB version requires schools to notify parents of the option of requiring written consent prior to release of the information. *Id.* § 7908(a)(2). In contrast, the Defense Authorization Act version requires that the student or parent specifically request that access be denied to military recruiters without prior consent. 10 U.S.C. § 503(c)(1)(B).

181. The first effort the military negotiated was access to higher education institutions with the Solomon Amendment. See 10 U.S.C. § 983. See generally *The Solomon Amendment: A Guide for Recruiters and Student Records Managers*, in LEGAL COMPENDIUM, *supra* note 125, at 601 (on file with the NEBRASKA LAW REVIEW). That effort was controversial, especially when the Armed Forces sent JAG recruiters to law schools. See Roberto L. Corrada, *Of Heterosexism, National Security, and Federal Preemption: Addressing the Legal Obstacles to a Free Debate About Military Recruitment at Our Nation's Law Schools*, 29 HOUS. L. REV. 301

ment of these provisions provides campus access to military recruiters correlative to that access offered to higher education recruiters.

The threshold issue with this type of provision is how the military's right to access student records can be enforced. NCLB and the defense authorization legislation are clearly spending clause legislation, the rationale used by the Supreme Court in denying a private right of action under FERPA. Indeed, NCLB has already been interpreted to create no right of action.¹⁸² Thus, the military would have a hard time enforcing access other than through the usual administrative recourse of cutting off a public school's federal funding.

Another issue raised by these provisions is the government's *laissez-faire* attitude toward students' directory information and parental opt-out provisions in the face of opposing public opinion. The records are automatically given to a military recruiter *unless* the parent or student specifically exempts these records by requiring prior consent. Both family and student privacy concerns are involved because the student's information is, more often than not, the same information as the family's. What these provisions imply is that a governmental intrusion into confidential information takes priority over privacy. Increasing government intrusion runs counter to the public's current concerns of family privacy that call for greater governmental regulation over similar private-sector intrusions by both telephone and mail.¹⁸³ Given family privacy concerns of private-sector intrusions over matters more inconsequential than military recruitment, families should be allowed to opt in to this kind of intrusion rather than to opt out as currently set out in these provisions.

An opt-in option may also be militated by the religious concerns of the families whose children attend public school, especially

(1992). See generally Francisco Valdes, *Solomon's Shames: Law as Might and Inequality*, 23 T. MARSHALL L. REV. 351 (1998).

182. *Ass'n of Cmty. Orgs. for Reform Now v. N.Y. City Dep't of Educ.*, 269 F. Supp. 2d 338, 343–44 (S.D.N.Y. 2003) (holding that the NCLB creates no individually enforceable rights with regard to notification of problem schools and rights of transfer or to supplemental educational services). In any event, the military's threat to cut off funding to any law schools that ban recruiters requires that the decision to cut off funding come from the Secretary of Defense, and the authority of the Department of Defense to regulate such funding is problematic. See Corrada, *supra* note 181, at 365–68.

183. The October 9, 2002, DOE guidance is more than a little disingenuous, in this regard, when it states: "This type of student information, commonly referred to as 'directory information,' includes such items as names, addresses, and telephone numbers and is information generally not considered harmful or an invasion of privacy if disclosed." U.S. DEP'T OF EDUC., ACCESS TO HIGH SCHOOL STUDENTS AND INFORMATION ON STUDENTS BY MILITARY RECRUITERS, <http://www.ed.gov/policy/gen/guid/fpc/pdf/ht100902b.pdf> (last visited May 15, 2006) (emphasis added).

Quakers¹⁸⁴ and Mennonites. These religious denominations object to service in the military,¹⁸⁵ refusing even to register with the Selective Services as required of all eighteen-year-old males.¹⁸⁶ The intrusion of military recruiters by way of a school's disclosure of family information clearly interferes in perhaps the true legitimate privacy interest of the family unit.¹⁸⁷ A local educational agency better serves these students and families and their religious practices by allowing all parents to opt in to disclosure and access by the military.¹⁸⁸

H. Social Security Numbers

Section 7 of the Privacy Act of 1974¹⁸⁹ sets out the regulatory scheme for maintaining the privacy of social security numbers ("SSN"s) by all local, state, and federal agencies. A regulatory scheme of long standing, section 7 prohibits discrimination in government services for refusal of an individual to disclose her SSN except under federal statute or a pre-1975 statutory scheme. Any request for an SSN must be accompanied by a notice that advises whether the request is mandatory or voluntary, the nature of the statutory mandate requiring such disclosure, and the uses for the number. For privacy pur-

184. See, e.g., The Religious Society of Friends, Peacemaker Sites, <http://www.quaker.org/#6a> (last visited May 15, 2006).

185. Indeed, conscientious objectors are exempted from combatant duties. 50 U.S.C. app. § 456(j) (2000). See generally Jose de Sousa e Brito, *Political Minorities and the Right to Tolerance: The Development of a Right to Conscientious Objection in Constitutional Law*, 1999 BYU L. REV. 607.

186. See, e.g., *United States v. Schmucker*, 815 F.2d 413 (6th Cir. 1987) (involving a Mennonite seminary student who refused to register with the Selective Services); see Christine Hunter Kellett, *Draft Registration and the Conscientious Objector: A Proposal to Accommodate Constitutional Values*, 15 COLUM. HUM. RTS. L. REV. 167 (1984); Paul M. Landskroener, *Not the Smallest Grain of Incense: Free Exercise and Conscientious Objection to Draft Registration*, 25 VAL. U. L. REV. 455 (1991); Elizabeth Reilly, "Secure the Blessings of Liberty": A Free Exercise Analysis Inspired by Selective Service Nonregistrants, 16 N. KY. L. REV. 79 (1988). One Quaker who worked as a "window clerk" for the United States Postal Service went so far as to request that he be reassigned so that he could avoid having to assist visitors who came to the post office to register for the Selective Services registration. See *Garman v. U.S. Postal Serv.*, 509 F. Supp. 507, 508 (N.D. Ind. 1981).

187. The military has also engaged in a concerted campaign to persuade state legislatures to enact comparable access legislation. See, e.g., ALA. CODE § 16-1-25 (LexisNexis 2001); CAL. EDUC. CODE § 49603 (West 1993); IND. CODE § 20-10.1-29-3 (2000).

188. To do otherwise, by only allowing parents to opt-out, a school analogizes military recruitment with nonconsensual disclosure of routine information in a school yearbook. In addition to treating military recruitment as a less serious venture, Congress is treating it as a "routine use" of the information when in reality, disclosure in a school yearbook has more educational function, and is therefore a routine use.

189. 5 U.S.C. § 552a note (2000).

poses, most educational agencies these days use alternative student identification numbers rather than SSNs.¹⁹⁰

I. School Lunch Programs

One last privacy program that deserves mention is the National School Lunch Program.¹⁹¹ Similar to other federal privacy regimes, like HIPAA, the school lunch program confidentiality directives are fairly inflexible regarding whether or not to divulge confidential information. Local educational agencies are best served by following the advice of legal counsel and the directives of the United States Department of Agriculture ("USDA") in putting together a local privacy policy.¹⁹² Student eligibility for free and reduced-price breakfasts and lunches requires the compilation of sensitive student and household information, including all sources of income (welfare, unemployment compensation, and the like), SSNs of the applicant-adult, and food stamp information.¹⁹³ The types of information that can be disclosed—all eligibility information versus eligibility status only—and the types of consent required depend upon the governmental agency administering the related program. Such programs include education programs, Medicaid, State Children's Health Insurance Programs ("CHIP"s), and federal, state, and local enforcement laws.¹⁹⁴

Any violation of these confidentiality regulations is subject to criminal sanctions.¹⁹⁵ Security measures require that only persons with a direct connection to the lunch program may have access to this information.¹⁹⁶ All other disclosures may be made only upon requiring written parental consent with clear identification of the information that will be shared and with whom and providing the option to pick and choose the programs with which the educational agencies may share information.¹⁹⁷ Because the disclosure, access, collection, maintenance, and use protocols for this information are so narrow and are

190. See FORUM GUIDE, *supra* note 8, at 21 (noting that educational institutions can use an alternative identification number when a parent objects to the use of her children's social security numbers for identification).

191. 42 U.S.C. §§ 1751–1770 (2000 & Supp. II 2002).

192. See generally U.S. DEP'T OF AGRIC., ELIGIBILITY GUIDANCE FOR SCHOOL MEALS MANUAL (2001), http://www.fns.usda.gov/cnd/Guidance/eligibility_guidance.pdf [hereinafter ELIGIBILITY GUIDANCE] (providing "information on Federal policy regarding the determination and verification of students' eligibility for free and reduced priced meals in the National School Lunch Program and the School Breakfast Program"); see also FORUM GUIDE, *supra* note 8, at 19–20.

193. 7 C.F.R. § 245.2(a-4) (2005).

194. 42 U.S.C. § 1758(b)(2)(C); 7 C.F.R. § 245.6(e). The USDA has developed a helpfully detailed chart of the disclosure rules. See ELIGIBILITY GUIDANCE, *supra* note 192, at 50.

195. 42 U.S.C. § 1758(b)(2)(C)(v).

196. *Id.* § 1758(b)(2)(C)(iii); FORUM GUIDE, *supra* note 8, at 19.

197. ELIGIBILITY GUIDANCE, *supra* note 192, at 54.

limited to aid recipients, a local policy should be formulated and published, but the individual situational notices could be limited to those who apply for assistance.

III. THE NUTS AND BOLTS: THE PROTECTED INFORMATION AND ITS USES

When drafting a local educational policy, the drafters must determine the substance of the policy's protections. Inherent in that determination is what information should be protected in light of both the constitutionally protected right to informational privacy and the sometimes-nonconforming federal statutes and regulations.¹⁹⁸ At the very basic level, schools compile information and keep records for two reasons. The first reason is to sustain the schools' governmental function: recordkeeping is an administrative function arising from its governmental status. The second reason for maintaining records is because schools are makers and collectors of a plethora of material in their educational function. They make decisions about children and their educational progress, but in order to do so must establish enough context—i.e., collect enough information—about the students to help them reach their fullest educational potential.¹⁹⁹ Any local privacy policy must address both types of information and their collection, use, and disclosure. The following should inform the basic floor of any local policy and practice concerning educational information.

A. Collection and Maintenance of Government Information

Schools as government entities must collect information that maintains the viability of the institutions as state agencies. Information gathered in this role necessarily implicates the collection of personally identifiable information on students and their families so as to receive government funding by accounting for student attendance, to keep track of students' individual and comparative progress, and to compile basic health and safety information for its *in loco parentis* role over minors. The *routine use* of such information should be confined to these purposes. The Privacy Act of 1974 is instructive on the limits of the maintenance and collection of such information. Just the minimal information necessary for the government to function should be maintained, and the individual from whom the information is gleaned must be advised of the purpose for disclosing such information.²⁰⁰

198. State statutes and constitutional provisions may be even more stringent. See generally Stuart, *supra* note 9.

199. Although somewhat dated, *The Report of the Privacy Protection Study Commission* has a comprehensive and businesslike summary of the role and problems of recordkeeping in schools. See PRIVACY REPORT, *supra* note 69, at 397–98.

200. 5 U.S.C. § 552a(e) (2000).

Samples of the governmental acquisition of student information can be found in the DOE's comprehensive on-line *Nonfiscal Data Handbook for Early Childhood, Elementary, and Secondary Education*.²⁰¹ For students, such routine uses would cover collection of attendance and residence data for state and federal funding, emergency information, routine personal statistics and contact information, enrollment and attendance records, health conditions, and the like.²⁰² Despite the bureaucratic nature of the collection, this information should be routinely protected from disclosure that does not accord with the purpose for collection.

Because of the bureaucratic nature of such collection, maintenance and use of such records that more clearly "belong" to the local educational agency, a local privacy policy probably should not even formulate a protocol except with regard to otherwise protecting personally identifiable information from access and disclosure.

B. Collection and Maintenance of Educational Information

1. Protection of Student-"Owned" Information

What is more critical is a local policy dealing with informational privacy protocols for student-"owned" information. Distinct from a school's bureaucratic information-collection function is the school's educational function in which it collects and maintains information that belongs not to the school but to the student. A parent might exercise, on behalf of a minor child, some access to and control over that information, but the privacy right inherent in that personal information belongs to the child.

First and foremost is the tenet that informational privacy is personal to and belongs with the individual students, not their parents. One of the bizarre features of FERPA is the notion that, until a student turns eighteen years old, her parents are treated as the "owners" of the records. Upon reaching eighteen, the student "owns" her records and can prohibit parental access. In any privacy policy for public school students, parents may act as representatives for their children in matters beyond their maturity but should not have pre-

201. NAT'L CTR. FOR EDUC. STATISTICS, U.S. DEPT OF EDUC., *NONFISCAL DATA HANDBOOK FOR EARLY CHILDHOOD, ELEMENTARY, AND SECONDARY EDUCATION*, <http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2003419> (last visited May 15, 2006) [hereinafter NCES, DATA HANDBOOK]. This *Data Handbook* is an extensive on-line guide for the collection of various kinds of data by schools. Student data is dealt with in the "Student Domain" portion of the *Handbook*. It also covers other educational data areas, such as staff personal information and individual school recordkeeping. The DOE has made the *Data Handbook* easily accessible for discrete types of data recording. See NAT'L CTR. FOR EDUC. STATISTICS, *HANDBOOKS ONLINE*, <http://nces.ed.gov/programs/handbook> (last visited May 15, 2006).

202. NCES, DATA HANDBOOK, *supra* note 201, at on-line index.

sumed ownership rights over that information. As the child nears eighteen, she might have personal reasons why she would want to "own" her personal information exclusive of her parents. Such rights do inure to mature minors in decision-making privacy, and at least one privacy statute—COPPA—specifically accounts for certain decisions fourteen- to eighteen-year-olds may make. Consequently, the formulation of local school privacy policies must account for those distinctions, or at least make the parental representative status a matter of choice and not a limiting matter of law. Parents might have coextensive rights and responsibilities, but students should not be cut out of the rights to access and disclosure entirely, as current statutes allow.

A policy that acknowledged such student "ownership" over educational information would also implicitly prohibit schools from disclosing school records for any purposes, even to law enforcement, without prior notice to someone. Children's education information does not belong to the schools to turn over to individual law enforcement agencies with little probable cause and court supervision. The juvenile justice system need not provide all due process rights to minors, but the right against self-incrimination still remains one that courts recognize. So the first consideration in any locally drafted privacy policy—that students have rights in their own information—would prevent the disclosure of information without following proper subpoena procedures.

A local policy should also recognize that minors' school records are outside the purview of any state's open records act, except insofar as statistical information is necessary for accountability purposes. If the school is not the "owner" of the education information but only the safe depository, the information is not a government record subject to disclosure upon request and is even outside a reporter's request under the First Amendment. There is little to suggest that either the public or the press has any interest in this private information, especially regarding minors and even regarding disciplinary matters. Just as confidentiality is sacrosanct in juvenile justice proceedings, so too should it be in education records. It would be illogical for the public and the press to get disciplinary information from schools through the back door via an open records request that could not otherwise be accessible in related juvenile proceedings.

The same protections should hold true, contrary to FERPA, for any local educational agency that has a law enforcement arm of any local school agency, such as the Bureau of Safety and Security in Chicago.²⁰³ The protection of disciplinary information is even more im-

203. Chicago Public Schools, Safety & Security, <http://www.cps.k12.il.us/AboutCPS/Departments/SafetyandSecurity/safetyandsecurity.html> (last visited May 15, 2006). Such concerns should not to be confused with the right to get records from university police departments involving students who are not minors.

portant in disciplinary procedures that are more education-oriented than police-oriented proceedings, with different goals and educational outcomes.²⁰⁴ The use of student courts to impose discipline should be so protected. Thus, local school policies and internal protocols for discipline should be more rigorously protected than otherwise suggested by extant federal law by acknowledging the appropriate ownership of the information.

2. *The Scope of Protected Education Information*

Despite its problems, FERPA remains a good starting point for a local committee to determine what is protected information owned by students and covered by principles of informational privacy. As a base-line, FERPA's terminology of "education records" is adequate to the task. FERPA now defines "education records" as "those records, files, documents, and other materials which . . . contain information directly related to a student[] and are maintained by an educational agency or institution or by a person acting for such agency or institution."²⁰⁵ A "record" means "any information recorded in any way, including, but not limited to, hand writing, print, computer media, video or audio tape, film, microfilm, and microfiche."²⁰⁶ Thus, with few exceptions, just about everything that has been compiled by, about, or on behalf of a student as an education client (and not as a government client) is an education record.²⁰⁷ The few exceptions are not informa-

204. Rosenzweig, *supra* note 48, at 470-74. "Publicizing records of internal campus disciplinary hearings 'perpetuates the myth that a student code violation is a breach of the "law" with procedures that mimic the criminal court system.'" *Id.* at 470.

205. 20 U.S.C. § 1232g(a)(4)(A) (Supp. II 2002). This rather cursory definition supplanted a much longer definition in FERPA's original incarnation. Daggett & Huefner, *supra* note 12, at 13.

206. 34 C.F.R. § 99.3 (2005).

207. There are some obvious exemptions for items that are not, and should not be, otherwise accessible by parents or students nor subject to FERPA's disclosure provisions:

(i) records of instructional, supervisory, and administrative personnel and educational personnel ancillary thereto which are in the sole possession of the maker thereof and which are not accessible or revealed to any other person except a substitute;

(ii) records maintained by a law enforcement unit of the educational agency or institution that were created by that law enforcement unit for the purpose of law enforcement;

(iii) in the case of persons who are employed by an educational agency or institution but who are not in attendance at such agency or institution, records made and maintained in the normal course of business which relate exclusively to such person in that person's capacity as an employee and are not available for use for any other purpose; []

(iv) records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education [pertaining to medical treatment].

tion that a student or a parent would assume is "owned" by the student or that would be protected by their informational privacy rights: informal teacher-compiled information, law enforcement information, employee records, and records of students who have turned eighteen.²⁰⁸

By adopting a bright-line definition of an education record, a local policy should not limit the purview of informational privacy to tangible items. Oral information passed from a student to a teacher or counselor, and not otherwise considered documented, should also be kept confidential unless there are health and safety reasons that require it be divulged to the authorities. To the extent that students often view educational personnel as their only confidants, teachers and other professionals should keep such matters in trust when the law does not otherwise impose a duty for health and safety purposes.

20 U.S.C. § 1232g(a)(4)(B). An additional exemption is found in the regulations: "[r]ecords that only contain information about an individual after he or she is no longer a student at that agency or institution" are not included in the definition of "education record." 34 C.F.R. § 99.3. *But see* 20 U.S.C. § 1232g(a)(4)(B) (not including the fifth exemption).

208. The FERPA regulation that attempts to exempt "sole possession" records from education records is faintly ridiculous: "Records that are kept in the *sole possession* of the maker, are used only as a personal memory aid, and are not accessible or revealed to any other person except a temporary substitute for the maker of the record." 34 C.F.R. § 99.3 (emphasis added). As a practical matter, "sole possession" notes that are used "only as a personal memory aid" have no functional meaning to a teacher. Teachers often keep desk diaries, lesson plan notes, and the like that may or may not be shared with other school officials during the course of legitimate educational activities and would not otherwise be considered under the "ownership" of the student. Thus, teacher-generated exempted information should also include preliminary drafts of reports, personal folders of progress and observations, grade books, lesson plans and lesson plan books, and other information that is not intended to be "permanent" but are critical for the instruction of the student. This information is "owned" by the teacher and not the student, and certainly not the parents.

One eminently reasonable suggestion is

[t]hat [FERPA] be amended to make it permissible for records of instructional, supervisory, and administrative personnel of an educational agency or institution, and educational personnel ancillary thereto, which records are in the sole possession of the maker thereof, to be disclosed to any school official who has been determined by the agency or institution to have legitimate educational interests in the records, without being subject to the access provision of FERPA, provided, however:

- (a) that such records are incorporated into education records of the agency or institution or destroyed after each regular academic reporting period;
- (b) that such records are made available for inspection and review by a student or parent if they are used or reviewed in making any administrative decision affecting the student; and
- (c) that all such records of administrative officers with disciplinary responsibilities are made available to parents or students when any disciplinary decision is made by that officer.

PRIVACY REPORT, *supra* note 69, at 439-40.

Indeed, some states have adopted a confidentiality privilege for certain student communications.

However, there must be some commonsensical limits to what is or is not private information for students and to what is or is not worthy of constitutional protection, especially in everyday classroom activities. The outer limits necessarily must account for legitimate educational functions and the dual public-private nature of the educational arena. It also depends on the teaching style and the pedagogical rationale for engaging in public, private, and semi-public activities. Certain instruction necessarily takes place in front of others. Small group activities are semi-public while other activities—such as student discipline—are best kept private. There is nothing to suggest that some student somewhere is not going to be embarrassed by doing *anything* in public.²⁰⁹ However, the charge to local educational agencies is to try to define, perhaps locally, the kinds of legitimate and pedagogically sound activities that will not affect a student's informational privacy in ways that would be violative of those interests while still upholding its educational expectations.²¹⁰

209. The Supreme Court's having to deal with peer grading issues under FERPA clearly suggests this. See, e.g., Ronnie Jane Lamm, Note, *What Are We Making a Federal Case Of? An Interdisciplinary Analysis of Education and the Right to Privacy in the Classroom*, 18 *TOURO L. REV.* 819, 849–50 (2002).

210. Recently, the Tenth Circuit framed the privacy interest as a “legitimate expectation of privacy [in that information]” in determining that peer grading did not violate the Fourteenth Amendment. *Falvo v. Owasso Indep. Sch. Dist. No. I-011*, 233 F.3d 1203, 1208–09 (10th Cir. 2000), *rev'd*, 534 U.S. 426 (2002). That standard, as it pertains to children, is virtually unworkable because children do not necessarily have any “expectation” of privacy. The Tenth Circuit also got it wrong when it made light of the stigmatizing effect of grades by stating that, although “school work and test grades of pre-secondary school students constitute somewhat personal or intimate information, we cannot conclude that these grades are so highly personal or intimate that they fall within the zone of constitutional protection.” *Id.* at 1209. Lawyers and others who have typically experienced academic success are hardly in a position to declaim that students in general should not take grades so “personally” nor be embarrassed by them. See *Herndon v. Chapel Hill-Carrboro City Bd. of Educ.*, 899 F. Supp. 1443, 1454 (M.D.N.C. 1995) (“A student's choice of projects and reaction to those projects does not reveal such intimate or personal information that would give rise to a reasonable expectation of privacy.”), *aff'd*, 89 F.3d 174 (4th Cir. 1996).

The reality is that it is naïve to think that children do not already have some idea about their classmates' abilities without actually knowing private information revealed by grades. Children are astute observers of those classmates who, for example, receive individualized instruction, leave the classroom to attend extra sessions in resource rooms for the learning disabled, have been mainstreamed, attend sessions with Chapter I reading instructors, or are grouped by ability. Although the grades are clearly private information, the stigmatizing public information is already pretty well known. That is not to suggest that there has been a “waiver” of the privacy in that information; most teachers minimize the stigmatization of “shared” information through peer grading, student distri-

3. *Defining Student Permanent Records*

Starting from the baseline FERPA definition and accounting for the exceptions as discussed above, a local educational agency should also draft an education informational privacy policy that delineates what information should be maintained as a permanent record of the school, how much information should be collected, and how that information should be purged periodically.²¹¹

First, permanent, cumulative records of students contain information worthy of constitutional protection and often kept "in perpetuity." Depending upon the agency's recordkeeping, this cumulative record might be a repository for both government and educational purposes and could include bureaucratically collected information as well as educationally collected information, such as personally identifiable information, attendance records, grades and standardized test scores, and academic work.²¹² Standardized test scores would include not only achievement tests but the administration of any IQ and aptitude tests. These records might also include discipline records,²¹³ IDEA documentation, necessary health and safety information for the protection of the child as well as state-mandated information, such as immunizations, and a collection of parental authorizations.²¹⁴ Although permanent records are often kept "permanently" in one central filing location, IDEA documentation as well as related health and disability information should be kept in a more secluded, less accessible location.

Second, some education information need not be accumulated in a formal record but could be. Such information includes verified and accurate information on academic matters and, perhaps, counseling issues (including family background information), personality and in-

bution of graded work, limited access student folders, and knowing whom to "trust" with that information.

211. Primarily at stake are records of student information kept by the institution as an educational institution. *Owasso Indep. Sch. Dist. No. I-011 v. Falvo*, 534 U.S. 426, 431-32, 435 (2002). However, such permanent records kept by the institution *qua* educational institution should not be considered one set of records only or under only one "central custodian." Education records could be scattered in various parts of a school and still be protected private information, regardless of the custodian. Of particular concern are the "locations" and custodians of computerized records. See, e.g., O'Donnell, *supra* note 69, at 696-98.
212. RUSSELL SAGE FOUND., GUIDELINES FOR THE COLLECTION, MAINTENANCE AND DISSEMINATION OF PUPIL RECORDS 20, 48 (1970). The NCES's *Data Handbook* merges both government and education information in the maintenance of student records. See NCES, DATA HANDBOOK, *supra* note 201. School administrators likely do not always perceive the distinction between maintenance of bureaucratic information and safekeeping of student information.
213. A local policy might also adopt a purging protocol for discipline records in permanent files.
214. PRIVACY REPORT, *supra* note 69, at 399.

terest inventory results, extracurricular activities, honors and awards, and other such "nonessential" information about the student that is not necessary for health and safety nor for the proper function of the school.²¹⁵ Schools always generate this kind of information and should afford it the same protections as a permanent record, but it should not be kept in perpetuity. This type of information is useful for education personnel to keep track of students and to assist in their long-term achievement but has a limited life-span. Such information might be purged periodically.

The last category of information that could be put in a permanent cumulative record is accumulated at the local educational agency's discretion and also should be purged periodically. This information consists of both verified and unverified sensitive information dealing with the student's progress that may be essential for a long-term prognosis but is most especially necessary for short-term investigative purposes. This information should be purged as it is updated and evaluated for its long-term usefulness and accuracy in dealing with "academic performance, work habits, strengths and weaknesses, conduct, motivation, special problems, and the like." These records might include teacher and counselor observations, reports from outside agencies, work samples, and reports from parent-teacher conferences.²¹⁶

Protected information that would likely *never* go into an official student cumulative file are those files that are confidential as a matter of law. This information is usually exempt from third-party access and forbidden from disclosure, usually by either common law or statutory privilege. Such information includes the files of school psychologists, social workers, counselors, and perhaps even school nurses. These professionals are trained in recordkeeping and, often, are required to keep files for ethical reasons. Such files might include notes, transcripts, diagnoses, and test results; however, unless the "client" consents to disclosure, she is considered outside the purview of FERPA's education records,²¹⁷ though IDEA has provided very limited access and disclosure of such information.

The foregoing serves only a broad-brushed outline for a local education policy covering information that must be protected as a matter of law. Additional protected documentation or documents in a student cumulative record may vary from locale to locale so the list cannot necessarily be considered exclusive.²¹⁸

215. RUSSELL SAGE FOUND., *supra* note 212, at 20-21, 48.

216. *Id.* at 21-22, 48.

217. *Id.* at 22.

218. Common sense would, however, dictate that some "documents" are clearly not educational records because they are not "maintained" in a "filing cabinet in a records room at the school or on a permanent secure database." Owasso Indep.

C. Acceptable Use of, Access to, and Disclosure of Student Education Information

The constitutional limits on the use of and access to student information is that, except under very limited circumstances, consent should be required, whether from parents (in the appropriate case) or from the student. Obviously, the primary exemption for a local privacy policy is that nonconsensual disclosure can be made to a third party for health and safety reasons.²¹⁹ Even under those circumstances, the local policy should encourage all efforts to notify the student and her parents of that request.²²⁰ Otherwise, an educational agency's nonconsensual use of and access to education information should be limited to its "routine use."

The "use" of a record is, in reality, a type of disclosure of a record.²²¹ And "routine use" of a record is presumed valid without the consent of the individual.²²² Educational records should only be used for those purposes for which they were collected, as other government records are protected by the Privacy Act of 1974.²²³ A routine use is "for a purpose which is compatible with the purpose for which it was collected."²²⁴ A routine use for student education information clearly involves a "legitimate educational interest."²²⁵ Such an interest sets the practical limits on both the use of and access to information. The exact boundary to such legitimate pedagogical concerns "is primarily the responsibility of parents, teachers, and state and local school officials."²²⁶ Those uses include in-house use by education personnel at

Sch. Dist. No. I-011 v. Falvo, 534 U.S. 426, 433 (2002); see also Kelly A. Nash, Note, *Peer Grading Outlawed: How the Tenth Circuit Misinterpreted the Family Education Rights and Privacy Act in Falvo v. Owasso Independent School District*, 229 F.3d 956 (10th Cir. 2000), 25 HAMLINE L. REV. 479, 512-13 (2002).

219. 20 U.S.C. § 1232g(a)(1)(I) (Supp. II 2002).

220. Health and safety concerns are among the few applicable exemptions that derive from the Privacy Act of 1974 and would also apply to educational information. 5 U.S.C. § 552a(b)(8) (2000). The majority of such situations that would require nonconsensual disclosure would involve health records and emergency contact information contained in the bureaucratic files, not in the students' education information such as grades or test results. A good central office of any school is familiar with the needs of medically fragile children or otherwise has an implicit understanding that parents will be contacted in case of emergency; notification procedures are already in place and likely do not afford access by anyone other than central office personnel.

221. See, e.g., *id.* § 552a(a)(7) (defining "routine use").

222. 20 U.S.C. § 1232g(b)(1); see also 5 U.S.C. § 552a(b)(3).

223. See, e.g., 5 U.S.C. § 552a(a)(7), (b)(3); see also Project, *Education and the Law: State Interests and Individual Rights*, 74 MICH. L. REV. 1373 (1976).

224. 5 U.S.C. § 552a(a)(7).

225. 20 U.S.C. § 1232g(b)(1)(A).

226. Hazelwood Sch. Dist. v. Kuhlmeier, 484 U.S. 260, 273 (1988); see also Larson v. Indep. Sch. Dist. No. 361, Nos. Civ.02-3611(DWF/RLE), Civ.02-4095(DWF/RLE), 2004 WL 432218, at *7 (D. Minn. Mar. 2, 2004) (involving a local policy which

that institution for the educational interests of the student²²⁷ as well as use by federal and state education agencies for educational purposes. Even so, the local policy should require a record of who has "routine-use" access, except perhaps in-house use.

Educationally related uses—or routine uses—that do not require consent could follow the fairly narrow categories of "routine users" set out by FERPA:²²⁸ (i) school officials with "legitimate educational interests" in the records; (ii) school officials of transferee educational institutions; (iii) state and federal agencies for audit and reporting purposes; (iv) entities involved with student financial aid; (v) organizations involved in student testing and instructional materials; and (vi) accreditation organizations. These routine uses include: the performance of the tasks for which the school official was hired; the fulfillment of official business of the educational agency; the accomplishment of tasks concerning a student; and purposes consistent with the maintenance of the information.²²⁹ And regardless of any other statute, IDEA limits access to these educational uses.²³⁰

One category of routine user is flexible, and that category concerns the local agency's denomination of school officials who have a "legitimate educational interest" in the information. IDEA clearly limits that interest to those who are involved in providing educational services under the statute. However, this restriction does not seem to affect the power of the educational agency to define the appropriate school officials under FERPA.²³¹ The DOE has suggested—and apparently some educational agencies have adopted²³²—the following general criteria for defining which routine users may have access to educational records: (i) regular educational employees of the agency (e.g., teachers, administrators, counselors, and so forth); and (ii) "persons employed by or under contract to the agency or school to perform a special task."²³³ These straightforward definitions or something similar would clearly inhabit a local policy.

defined school personnel qualified to receive student information pursuant to FERPA).

227. See, e.g., *M.R. ex rel. R.R. v. Lincolnwood Bd. of Educ.*, Dist. 74, 843 F. Supp. 1236 (N.D. Ill. 1994), *aff'd*, 56 F.3d 67 (7th Cir. 1995).

228. 20 U.S.C. § 1232g(b)(1).

229. FORUM GUIDE, *supra* note 8, at 51.

230. Consent is required if the education records are used for anything but an educational purpose. 34 C.F.R. § 300.571(a)(2) (2005). In addition, IDEA regulations restrict the "routine use" of education records to "participating agencies." *Id.* § 300.571(b). A "participating agency" is "any agency or institution that collects, maintains, or uses personally identifiable information, or from which information is obtained . . ." *Id.* § 300.560(c).

231. 20 U.S.C. § 1232g(b)(1)(A).

232. E.g., *Larson v. Indep. Sch. Dist. No. 361*, Nos. Civ.02-3611(DWF/RLE), Civ.02-4095(DWF/RLE), 2004 WL 432218, at *7 (D. Minn. Mar. 2, 2004).

233. FORUM GUIDE, *supra* note 8, at 51.

On the other hand, all disclosures to law enforcement or pursuant to some other legal order are not within a routine use but may instead require special treatment for appropriate use and access. If the information is compiled for administrative purposes and belongs to the school as a government agency, every effort should be made to redact personally identifiable information before handing over education information. However, if the requested information is collected for educational purposes and belongs to the student, a local policy should require greater care be given to protect the rights of students than those afforded by the federal statutes.

Any local policy must recognize that FERPA requires students and parents to be notified before personally identifiable information is released or made accessible pursuant to court order.²³⁴ Such provision is in tune with procedural rules for service of requests for production of documents, response to subpoenas duces tecum,²³⁵ and appropriate service of discovery requests on parties. Regardless of whether the educational agency is served as a party²³⁶ or whether the educational agency is served with a third-party request for production or subpoena duces tecum,²³⁷ notice must be given to the affected students and parents with an appropriate time for the students and parents to respond.

However, a local policy runs afoul of the Fifth Amendment if it adheres to FERPA's allowance for release of educational records without notice pursuant to federal grand jury and other law enforcement subpoenas.²³⁸ Similarly problematic is FERPA's "routine use" that allows nonconsensual disclosure to juvenile justice systems under state statutes authorizing such a disclosure.²³⁹ "[T]he government's inter-

234. 20 U.S.C. § 1232g(b)(2)(B).

235. FED. R. CIV. P. 45; *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 581 (3d Cir. 1980).

236. *See Mann v. Univ. of Cincinnati*, 152 F.R.D. 119, 120–21, 126 (S.D. Ohio 1993) (holding that the university violated a student's privacy rights when it accessed her medical records held by the student clinic without the student's knowledge and before the due date on subpoena). *But see United States v. Bertie County Bd. of Educ.*, 319 F. Supp. 2d 669, 671 (E.D.N.C. 2004) (ordering the school board to turn over personally identifiable student information to the United States government pursuant to a civil request for production of documents because FERPA is not violated when the government is acting in a law enforcement capacity).

237. Under some circumstances, written consent or, at the very least, the option of waiving consent, might be required. *Westinghouse*, 638 F.2d at 581. *But see Bertie County Bd. of Educ.*, 319 F. Supp. 2d at 671.

238. 20 U.S.C. § 1232g(b)(1)(J).

239. *Id.* § 1232g(b)(1)(E). The goal—better delivery of services to children at risk of delinquency—is laudable:

FERPA allows schools to play a vital role in a community's efforts to identify children who are at risk of delinquency and provide services prior to a child's becoming involved in the juvenile justice system. . . . As more and more States establish information sharing programs to serve students through cooperation with the juvenile justice system, the emphasis on neighborhood school participation in interagency information

est in securing evidence for law enforcement, although compelling, is not absolute and must be balanced against the court's recognition of the Fifth Amendment's protection for individual privacy."²⁴⁰ A privacy interest in education information clearly belongs to the student who would have standing to assert a proprietary interest in the material just as would an adult in similar information. Indeed, a similar routine use was stricken from a federal agency's system procedures as an unlawful effort to circumvent the Privacy Act.²⁴¹ An educational agency treads on very shaky ground under the Fifth Amendment by *not* providing prior notice to affected students whose personally identifiable information and education records might be accessed by seemingly unlawful means.²⁴² Upon such notice, the student and parents at least have the opportunity to oppose the disclosure and require that the requesting party comply with applicable standards of relevance²⁴³ or otherwise require a judicial balancing of the government's need for the information with the student's right of privacy.²⁴⁴

Last, a local policy must limit tertiary access to and disclosures of information by individuals who have legal routine use of the informa-

sharing agreements will increase. FERPA need not be a barrier to this progress toward proactive information sharing networks.

OFFICE OF JUVENILE JUSTICE & DELINQUENCY PREVENTION, U.S. DEP'T OF JUSTICE, SHARING INFORMATION: A GUIDE TO THE FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT AND PARTICIPATION IN JUVENILE JUSTICE PROGRAMS 13 (1997), <http://www.ed.gov/policy/gen/guid/fpco/pdf/sharinginfo.pdf> [hereinafter OJJDP, SHARING INFORMATION]. However, laudable goals do not make such nonconsensual disclosure constitutional. Interestingly enough, the DOE has hidden guidance on this matter to obscure references in its *Forum Guide* under the heading "Release to Other Service Agencies," as if criminal procedures under the Constitution were not at issue but rather just another mundane and routine student service. FORUM GUIDE, *supra* note 8, at 76.

240. *In re Grand Jury Subpoena Duces Tecum* Dated May 9, 1990, 741 F. Supp. 1059, 1070 (S.D.N.Y. 1990) (citation omitted), *aff'd*, 956 F.2d 1160 (2d Cir. 1992).

241. *Doe v. Stephens*, 851 F.2d 1457, 1466-67 (D.C. Cir. 1988) (chastising the Veterans Administration for adopting a regulation that made disclosures of medical information a "routine use" in responding to a subpoena).

242. Educational agencies are ostensibly protected from liability for the disclosure of school records under the USA Patriot Act amendments to FERPA. See 20 U.S.C. § 1232g(j)(3). However, if an educational agency is aware of basic Fifth Amendment principles, it could hardly rely on this "protection" when it is not even a close question.

243. See, e.g., FED. R. CIV. P. 26(b).

244. *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 578 (3d Cir. 1980) ("The factors which should be considered in deciding whether an intrusion into an individual's privacy is justified are the type of record requested, the information it does or might contain, the potential for harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record is generated, the adequacy of safeguards to prevent unauthorized disclosure, the degree of need for access, and whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access.").

tion. The most constitutionally consistent policy forbids further disclosure in the absence of consent. In addition, FERPA mandates that any and all disclosures to outside agencies come with an implicit, if not explicit, tertiary promise of confidentiality, the promise not to reveal personally identifiable information to anyone outside the requesting entity;²⁴⁵ "personal information shall only be transferred to a third party on the condition that such party will not permit any other party to have access to such information without . . . written consent."²⁴⁶ Thus, to be on the safe side, a local privacy policy must require all third parties to whom records are disclosed to agree not to make any further disclosure.

D. Reformulating Directory Information

A local policy should also reserve a particular category for directory information because current policies under FERPA go far beyond the legitimate educational purposes that should otherwise limit its disclosure. Directory information is personally identifiable information that an educational agency can regularly disclose without parental consent. Local educational agencies could allow such disclosure after the appropriate notice to parents for legitimate educational purposes. The routine use of directory information should probably be limited to allow the disclosure of only minimal information for newspapers, yearbooks, athletic programs, and the like. The only information really needed for these educational uses is the student's name; photograph; participation in recognized sports and extracurricular activities; enrollment status; grade level; height and weight of athletic team members; and degrees, honors, and awards received.²⁴⁷

In addition, a local educational agency may decide to provide marketing information to commercial enterprises for which PPRA's guidelines on this matter are probably the most cogent. Any activities whereby personal information is collected, disclosed, or otherwise used for marketing, for sale, or for divulging lists to others for that

245. 20 U.S.C. § 1232g(b)(1)(E)(ii)(II) ("[T]he officials and authorities to whom such information is disclosed [must] certify in writing to the educational agency or institution that the information will not be disclosed to any other party except as provided under State law without the prior written consent of the parent of the student."); see also *id.* § 1232g(b)(1)(F).

246. *Id.* § 1232g(b)(4)(B). The educational agency may not permit access within five years of a violation. *Id.* However, there is some concern that this tertiary prohibition likely does not apply to directory information as FERPA is currently constructed.

247. There seems to be no principled reason for a school to routinely disclose without consent a minor student's address, telephone listing, date and place of birth, and e-mail address as currently espoused by the DOE and FERPA. In any case, PPRA categorizes much of this information as "personal information" for which a local policy can limit disclosure for marketing purposes. *Id.* § 1232h(c)(1)(E), (6)(E).

purpose²⁴⁸ require an even more simplified system of information. Acceptable pieces of personal information under PPRA are limited to the student's (or her parent's) first and last names, home address, and telephone number (which is optional).²⁴⁹ PPRA also has a fairly good list of the limits on educationally related nonconsensual disclosures of such information for educational products or services.²⁵⁰

Once the local school district designates what educational information to protect and to whom nonconsensual disclosure is an appropriate routine use, the district must engage in the detail-work of complying with the Constitution and the multifarious federal statutes.

IV. "PEACEABLE LIVING ONE AMONGST ANOTHER":²⁵¹ DRAFTING A LOCAL POLICY

A. The Drafters and the Draft

Each educational agency should have a privacy policy in place that, in the main, deals with the protections over educational information.²⁵² That policy should be maintained for implementation and training in faculty handbooks, for annual distribution in a parent-student handbook,²⁵³ and, if applicable, on the school district's website.

Why a local policy? Because Congress is unlikely to cure the statutory problems any time soon. Local educational agencies are left to weather the increasingly imaginative civil rights and constitutional claims as plaintiffs find no relief in pursuing the limited and rarely

248. *Id.* § 1232h(c)(2)(C).

249. *Id.* § 1232h(c)(6)(E). PPRA does not make the telephone number optional; however, with new federal and state "do-not-call" lists, a school would be hard-pressed to justify requiring the dissemination of telephone numbers. Likewise, PPRA's listing of SSNs is unlawful without stringent limitations.

250. "Educational products or services" include postsecondary recruiters, book clubs and other literary programs, curriculum and instructional materials, certain testing and assessment instruments, student-recognition programs, and school-related sales activities. *Id.* § 1232h(c)(4)(A). Only PPRA's allowance of military recruitment might run afoul of appropriate nonconsensual disclosure of directory information.

251. JOHN LOCKE, TWO TREATISES OF GOVERNMENT 163 (Mark Goldie ed., Everyman 1993) (1690) ("The only way whereby anyone divests himself of his natural liberty, and puts on the bonds of civil society is by agreeing with other men to join and unite into a community, for their comfortable, safe, and peaceable living one amongst another, in a secure enjoyment of their properties, and a greater security against any that are not of it.").

252. See generally FORUM GUIDE, *supra* note 8; see also Scott A. Gartner, Note, *Strip Searches of Students: What Johnny Really Learned at School and How Local School Boards Can Help Solve the Problem*, 70 S. CAL. L. REV. 921, 965-68 (1997) (positing that local school boards and community constituents should be responsible for drafting guidelines for strip-search policies).

253. E.g., W. Bradley Colwell & Brian D. Schwartz, *Student Handbooks: A Significant Legal Tool for the 21st Century*, 154 W. EDUC. L. REP. 409, 415 (2001).

implemented statutory funding penalties. Local policies, rather than blind adherence to flawed federal directives, may forestall those suits by tightening up school district practices pursuant to constitutional guidelines while still maintaining some local control. The DOE is not getting sued for problems in its guidances—local educational agencies are. In addition, the local school board is the entity best equipped to provide security systems that are easily understandable, and local implementation of policies would greatly enhance the likelihood of providing for systemic accountability procedures.

The members of such a committee or commission concerning student privacy rights and responsibilities should ideally include teachers, administrators, parents, and perhaps students, especially students who are eighteen or older and whose records belong to them.²⁵⁴ The more the stakeholders believe they are vested in the policy, the more cooperation a school district will receive in the implementation of the policy because of better community understanding. Such local control would also be more sensitive to the informational needs of and differing interests in commercial disclosure and the school's legitimate interest in defining its own directory information.

The process of drafting a privacy policy should involve serious study of the extant law²⁵⁵ and, because the matter is one of constitutional dimensions, a sensitivity to the concerns of a minority viewpoint. Subsequent public hearings would be useful to examine that minority viewpoint.²⁵⁶ Sample policies might be examined,²⁵⁷ but so many of them are influenced by the incorrect and ineffectual advice offered by the DOE that they should be used guardedly. Hence, the school district's attorney should review any policy before the governing body adopts it.²⁵⁸ And the policy should be revisited by a commission every three or four years and reviewed annually by the district's attorney for changes in the law.²⁵⁹

To accomplish its purpose, any policy must be drafted with a few concerns in mind. First, the policy must be easily understood if for no other reason than practicality.²⁶⁰ Second, in keeping with the "plain

254. PRIVACY REPORT, *supra* note 69, at 436; RONALD W. REBORE, SR., A HANDBOOK FOR SCHOOL BOARD MEMBERS 173 (Prentice-Hall, Inc. 1984); *see also* Peter Sansom & Frank Kemerer, Comment, *It's All About Rules*, 166 W. EDUC. L. REP. 395 (2002) (suggesting that class officers should aid in writing student education codes so they are easily understandable to students). In any event, PPRa requires parental input for local policies. 20 U.S.C. § 1232h(c)(1).

255. REBORE, *supra* note 254, at 173–74.

256. *Id.* at 174.

257. *E.g.*, FORUM GUIDE, *supra* note 8, at 22–41, 64–69, 80–85.

258. Colwell & Schwartz, *supra* note 253, at 416.

259. *Id.*; REBORE, *supra* note 254, at 174.

260. For example, certain parental notices under IDEA must be "understandable," 34 C.F.R. § 300.504(c) (2005), thus assuring "informed" parental consent for certain due procedures, *id.* § 300.505(a). More specifically, IDEA requires local educa-

language" initiatives in government communications,²⁶¹ the same principles should be used for student handbooks, adult notices, and faculty compliance guides.²⁶² This is particularly so given the muddled state of privacy regulation over student education information.²⁶³ Third, a certain portion of the student population, those students who are eighteen or older, must be adequately notified of their privacy rights when their parents are no longer their representatives. With these points in mind, the committee must tackle the sensitive and complex points in the substantive privacy protections in the policy.

B. The Substance

As previously mentioned, FERPA and other applicable federal statutes contain some privacy protections that serve as the policy's absolute minimum. Where the federal statutes and regulations do not actually protect educational privacy or run afoul of the Constitution, the local educational agency must choose more restrictive and protective guidelines.

The following are nonnegotiable guidelines that must be included in any local policy:

1. Student information contained in education records is protected by the Constitution and requires consent before disclosure.
2. The educational agency must describe the records it holds.²⁶⁴
3. Students must have access to their own records within reason and, if necessary, under appropriate supervision.
4. Mature minor students have the right to withhold consent to disclosure of records.
5. Nonconsensual disclosure of education records is appropriate for the following educationally related purposes: internal access to authorized school officials; officials of transferee schools; authorized representatives of state and federal educational agencies; financial aid applications; organizations conducting educational research for predictive testing, student aid

tional agencies to send notices of records confidentiality and FERPA rights in parents' native language. *Id.* § 300.561(a)(1).

261. See, e.g., THOMAS A. MURAWSKI, *WRITING READABLE REGULATIONS* 112–18 (Carolina Academic Press 1999); Michael S. Friman, *Plain English Statutes: Long Overdue or Underdone?*, 7 LOY. CONSUMER L. REV. 103 (1995); Steven L. Schooner, *Communicating Governance: Will Plain English Drafting Improve Regulation?*, 70 GEO. WASH. L. REV. 163, 167–69 (2002).

262. See, e.g., MURAWSKI, *supra* note 261, 100–03.

263. See Thomas F. Blackwell, *Finally Adding Method to Madness: Applying Principles of Object-Oriented Analysis and Design to Legislative Drafting*, 3 N.Y.U. J. LEGIS. & PUB. POL'Y 227, 228–34 (2000) (footnote omitted).

264. 34 C.F.R. § 300.565.

programs, and instructional improvement; and accrediting organizations.

6. Strictly defined directory information is disclosed without consent for intrascholastic and otherwise educationally related purposes.
7. Directory information for educationally related purposes consists only of name; photograph; age; major field of study; participation in officially recognized activities and sports; weight and height of members of athletic teams; grade level achieved; and degrees, honors, and awards received.
8. Social security numbers are not routinely requested and never disclosed except in compliance with the Privacy Act and any federal statutory protocol that requires their notation, such as the National School Lunch Program.
9. The educational agency complies with the minimum privacy guidelines under the PPRA concerning parental consent to surveys and physical examinations, but only to the extent those guidelines are constitutional.
10. Special education records are kept separate from the records of general education students. Medical information required for legitimate education purposes for administering the IDEA will be noted as available but stored apart from the education records.
11. Medical information of all students is not an education record, and any and all such information is kept segregated from education records.
12. The educational agency that falls within HIPAA must comply, including the appointment of a privacy officer.
13. Personally identifiable information and/or education records are disclosed only upon parental consent to military recruiters and marketing representatives.
14. Appropriate notice is given to students and parents before the following disclosures of personally identifiable information and/or education records: to law enforcement agencies; in compliance with any subpoenas or other requests for documents; and as required by any order of the court.
15. The local educational agency complies with students' privacy interests in all disclosures for bureaucratic rules and regulations concerning the governance of the agency, such as attendance reports, the National School Lunch Program Act, and the like.

16. The educational agency appoints an administrator to act as privacy czar in charge of the privacy regulations, access to records, security of records, and staff training.²⁶⁵
17. The educational agency adopts fair information practices to protect student informational privacy.

The policy should also have the following "negotiable" guidelines that could be included in a local privacy policy but would require both meaningful and effective notice to parents and students and their prior consent:

1. The policy defines "routine use" as "legitimate educational interest" and thus limits school officials who have nonconsensual disclosure and access rights.
2. The school enters into a compact with juvenile justice authorities and other social service agencies for disclosure with a parent-student opt-out provision.
3. The types of directory information are expanded but only with consent.
4. Directory information can be disclosed for commercial purposes, but only with consent.
5. Other disclosures of directory information are allowable if they would be beneficial to the school and/or the students so long as there is effective notice and prior consent.
6. Minor students are given the right to veto access to and disclosure of their educational records.
7. The local agency follows consent protocols under COPPA.
8. The policy defines the contents of education records and collection protocols.

Once the content can be established, then the local drafters must concern themselves with the fair information practices structure for the policy. This structure currently informs much of federal privacy policy-making.

C. Fair Information Practices

Any framework adopted by a local education agency should follow the long-recognized fair information practices ("FIP")s first formulated by the Department of Health, Education, and Welfare ("HEW") in 1973, to govern the collection, maintenance, and dissemination of sensitive information collected by that Department. These principles of

265. This privacy officer is *required* under both HIPAA and IDEA. *Id.* § 300.572(b). However, HIPAA compliance is less likely to be required as IDEA compliance. Congress also recently mandated each federal agency to appoint a Chief Privacy Officer "to assume primary responsibility for privacy and data protection policy." 5 U.S.C. § 552a note (2000); *see* Pub. L. No. 108-447, § 522, 118 Stat. 3268, 3268-70.

FIPs were initially set forth in a report by HEW entitled *Records, Computers, and the Rights of Citizens*,²⁶⁶ which addressed the increasing sophistication of computer-based recordkeeping. Several federal privacy statutes have tried to conform to these standards, including FERPA itself, with varying success.²⁶⁷

The original FIPs set out in the HEW report were as follows:

1. There must be no personal data record-keeping systems whose very existence is secret;
2. An individual must have an avenue to find out what information about him is in a record and how it is used;
3. An individual must be able to prevent information that was obtained for one purpose from being used or made available for other purposes without his consent;
4. An individual must be able to correct or amend a record of identifiable information about him;
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.²⁶⁸

More recently, the FTC issued a report to Congress for online privacy and simplified the appropriate FIPs as follows: Notice, Choice, Access, Security, and Enforcement:²⁶⁹

1. Prior Notice/Awareness principle: the agency advises the individual of the entity's collection, use, and disclosure practices vis à vis personal information;
2. Choice/Consent principle: the agency gives the individual the options for whether and how the personal information can be used;
3. Access/Participation principle: the agency gives the individual the right to inspect, review, and amend collected information;
4. Integrity/Security principle: the agency takes reasonable steps to assure accuracy of information and prevents unauthorized access;
5. Enforcement/Redress principle: the agency provides a means of ensuring compliance and/or "redressing" injuries.²⁷⁰

266. U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973), available at <http://www.aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm> [hereinafter HEW REPORT].

267. Winn, *supra* note 122, at 649–50. For example, HIPAA's regulations for the collection of protected health information incorporated three clearly identifiable fair information practices: (i) the patient has a right to inspect and to amend her records (access/participation); (ii) the provider must provide notice of its privacy practices and the use and disclosure of the information (prior notice/awareness); and (iii) the patient can request an accounting of the provider's disclosures (security and enforcement/redress). Gostin et al., *supra* note 129, at 1115, 1128–30.

268. HEW REPORT, *supra* note 266, at xx–xxi, available at <http://www.aspe.hhs.gov/datacncl/1973privacy/Summary.htm> (providing additional explanation of the HEW Report's recommendations).

269. See FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf> [hereinafter FTC, PRIVACY ONLINE].

270. Steven Hetcher, *The De Facto Federal Privacy Commission*, 19 J. MARSHALL J. COMPUTER & INFO. L. 109, 121–22 (2000); see HEW REPORT, *supra* note 266; Jerry Berman & Deirdre Mulligan, *Privacy in the Digital Age: Work in Progress*, 23 NOVA L. REV. 551, 557 (1999); Garber, *supra* note 158, at 153 n.109; Susan E.

Although not all student records are computer data records, these simplified data protections are useful for a local educational agency in drafting its own privacy policy.

1. Notice/Awareness Principle

Parents and children must be notified annually of the educational agency's privacy policy.²⁷¹ The annual distribution of student handbooks might suffice to give proper notice; publication in an annually distributed handbook would certainly provide an appropriate forum.²⁷² But the reality of parents actually reading a student handbook all the way through every year is probably overoptimistic, thereby not comporting with the "awareness" principle. Thus, the best opportunity to give personal and specific notice to each parent is during annual registration.²⁷³

Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1219 (1997); Gostin et al., *supra* note 129, at 1128-30 (describing fair information practices employed to protect personal health information). The first four FIPs are also specifically identified by the FTC as standards that private-sector websites should follow with regard to the collection of personally identifiable information. FTC, *PRIVACY ONLINE*, *supra* note 269.

Formalizing FIPS was suggested for the following purposes: (i) to prevent the accretion of secret personal data records held by the government; (ii) to provide a citizen the opportunity for finding out what information the government held and how it was being used; (iii) to allow a citizen to limit the disclosure of his personal information for purposes other than for which it was originally provided; (iv) to give a citizen the right to correct information being held; and (v) to force the government to keep accurate records and to prevent misuse. Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1165 (2002); see also Paul M. Schwartz, Comment, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559, 1561 (2000) (footnotes omitted).

271. Both FERPA and PPRA require annual notification. 20 U.S.C. §§ 1232g(e), 1232h(c)(2)(A)-(B) (Supp. II 2002); 34 C.F.R. § 99.7 (2005).

272. Colwell & Schwartz, *supra* note 253, at 414.

273. The DOE advises schools that the notification need not be made individually to parents or eligible students and instead suggests that local or student newspapers, handbooks, or similar avenues of "distribution" are sufficient; however, the DOE's advice is not realistically "effective" notice. See U.S. DEPT OF EDUC., FERPA GENERAL GUIDANCE FOR PARENTS, <http://www.ed.gov/policy/gen/guid/fpco/ferpa/parents.html> (last visited May 15, 2006); U.S. DEPT OF EDUC., FERPA GENERAL GUIDANCE FOR STUDENTS, <http://www.ed.gov/policy/gen/guid/fpco/ferpa/students.html> (last visited May 15, 2006). FERPA specifically requires that the annual notice "effectively informs" parents and eligible students. 20 U.S.C. § 1232g(e). The FERPA regulations and the DOE require only notice that is "reasonably likely to inform" general education students but must "effectively notify" special education parents and parents whose primary language is not English. 34 C.F.R. § 99.7 (emphasis added). Surely, providing notice that is not even designed to be "effective" is a practice and policy in violation of FERPA.

Because school districts are required to give notices and obtain consent under some statutes, such as COPPA, providing notice and acquiring consent at the same time would seem to be the easiest format and would allow school districts to get it all taken care of in one fell swoop. Annual registration (or registration upon entering a new school) as a precondition to matriculation would be the ideal time to distribute notices and obtain signed consent forms. Such notices could provide a truncated version of all the privacy rights and responsibilities of the school, parent, and child with references to the full policy in the student handbook or on the website. Attached but easily removed would be the consent forms that would be required for further disclosure of information. And although school administrators decry the perceived burden of paperwork,²⁷⁴ there would seem to be little administrative work in giving each parent, at the time of school registration, an individual notice with a checklist of notices and consents. As each child is then entered into each school's database, the appropriate sorting characteristics could be attributed to the parents' choices so that different lists could be generated.²⁷⁵

2. *Choice/Consent Principle*

Choice: The fair information practice of choice in education information would have to clearly distinguish, for both students and parents, those instances in which consent will not be required and those when it is. As described above, routine uses of information for educationally related functions would not require affirmative consent so the local privacy policy should delineate those records that will be accessible for educational purposes, under what circumstances, and by whom. Also, the nonconsensual disclosure of minimal directory information for educationally related purposes must be set out for appropriate notice. But any other use of education records—particularly any commercial use—and the expansion of the limits of directory information requires the parents to choose and supply affirmative consent.

*Consent:*²⁷⁶ As with adults' rights under the Privacy Act of 1974, student educational privacy rights must be governed by an affirmative consent system—an opt-in system rather than opt-out system.²⁷⁷ There is no philosophical, economic, nor logical justification for not doing so, especially because some privacy statutes protecting children,

274. PRIVACY REPORT, *supra* note 69, at 429.

275. "Situational" notices will also have to be sent under PPRA whenever an educational agency engages in the administration of surveys or physical examinations that are not otherwise scheduled at the time the annual notice is distributed. 20 U.S.C. § 1232h(c)(2)(C).

276. See also RUSSELL SAGE FOUND., *supra* note 212, at 25–28.

277. See, e.g., Garber, *supra* note 158, at 153 n.109.

such as COPPA and HIPAA, *require* affirmative opt-in consent from parents.²⁷⁸ An opt-in system gives the parent a reasonable opportunity to select how much of the child's privacy and even the parents' privacy should be revealed and presumes a protection of that privacy. Opt-out programs are problematic because they require meaningful and effective notice—something that is not currently required by the DOE—in order to make an informed choice to consent.²⁷⁹ And there is something very democratic about having an “opt-in” form of government where the participant believes he truly has a choice in the use of the information.²⁸⁰

A community privacy policy might also include interagency disclosure to juvenile justice authorities. Certain information-sharing practices are helpful in the administration of the juvenile justice system and to keep children out of it. Indeed, interagency cooperation would likely streamline services for children's supportive services, increasing

278. Under similar circumstances, parental consent is usually required before providing medical treatment to children, defined by one court as an associational privacy right. *Wallis v. Spencer*, 202 F.3d 1126, 1141–42 (9th Cir. 2000) (holding that a state must get prior consent before engaging in an investigative physical examination of children).

279. Hatch, *supra* note 160, at 1498–1500. The lure of opt-out systems is the merchant's “bet” that the consumer will not want to take the trouble to affirmatively “withdraw” consent. Unfortunately, most federal and state laws follow the opt-out type of system, and most consumers tend to stay with that “default” position. Vera Bergelson, *It's Personal but Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 393 (2003). That is especially so when the opt-out process is difficult. *Id.* at 394.

280. See, e.g., Marla Pollack, *Opt-In Government: Using the Internet to Empower Choice—Privacy Application*, 50 CATH. U. L. REV. 653, 653 (2001). To the contrary is the opinion in *U.S. West, Inc. v. F.C.C.*, 182 F.3d 1224, 1238–39 (10th Cir. 1999). In the *U.S. West* decision, the Tenth Circuit determined that an FCC regulation requiring that telecommunications customers affirmatively approve—or “opt-in”—to a company's use of “customer proprietary network information” violates the First Amendment regarding commercial speech and is insufficiently tailored to meet the government's goals of maintaining customers' privacy. *Id.* Of course, the problem was analyzed in a cost-benefit manner, disregarding entirely that utilities are government proxies. The consumer's giving information to a utility lacks much semblance of voluntariness because one must have a relationship with the utility and, in reality, there is very little real competition in a given jurisdiction. But see Michael E. Staten & Fred H. Cate, *The Impact of Opt-In Privacy Rules on Retail Credit Markets: A Case Study of MBNA*, 52 DUKE L.J. 745 (2003) (arguing that mandating opt-in privacy regulations on private entities costs too much).

Here, the better analogy is to the Privacy Act. If the federal government has an opt-in system for adults, how hard is it to ask the same of an educational agency? This opt-in system should not be confused, however, with the diminution of any rights mature minors themselves have in health and medical decision-making, like school condom-distribution programs, that otherwise pits parents' interests against their children's right to privacy. See, e.g., *Parents United for Better Schs., Inc. v. Sch. Dist. of Philadelphia Bd. of Educ.*, 978 F. Supp. 197, 209 (E.D. Pa. 1997), *aff'd*, 148 F.3d 260 (3d Cir. 1998).

access to social and educational services, and conducting policy planning.²⁸¹ However, “[a]gencies that collaborate for in-take procedures, direct service, or research should explicitly spell out procedures for obtaining written consent and define in advance what data will be shared, how they are used, and the means of ensuring privacy if they are released from the originating agency.”²⁸² Otherwise, there is no justification for exempting disclosures to the juvenile justice system from the required consent provisions that offer protections similar to those afforded adults under the rules of criminal procedure and due process.

In offering a Choice of Consent options on an annual basis, a local policy should be guided by the following:

1. No consent required:
 - A. Student use
 - B. Educationally related purposes (“routine uses”)
 - C. Disclosure of minimal directory information for intraschoolastic purposes
 - D. Access by parents (including noncustodial parents pursuant to the appropriate state law and court orders)
 - E. Emergencies
2. Annual opt-in (prior consent required):
 - A. Expanded selection of directory information
 - B. Commercial use of directory information
 - C. HIPAA
 - D. COPPA
 - E. Military recruitment
 - F. National School Lunch Program, if applicable
 - G. Access by noncustodial parents different from 1(D) above
3. Annual opt-out (prior consent presumed):
 - A. Use of directory information under any circumstances
 - B. PPRA
 - C. Juvenile justice and other social service agencies in a compact agreement that protects privacy
4. Situational opt-outs: PPRA (for data collection not otherwise contemplated at the time of the annual notification)

281. FORUM GUIDE, *supra* note 8, at 76. One such program is asserted to be the Serious Habitual Offender Comprehensive Action Program. OJJDP, SHARING INFORMATION, *supra* note 239, at 16–17.

282. FORUM GUIDE, *supra* note 8, at 76.

3. Access/Participation Principle

Access: The access practice in a local policy would obviously afford access rights to education records to parents, at least until the child is eighteen.²⁸³ Allowing parents such access seems appropriate as they are the guardians with the best ability to assure a child's due process rights are protected and that her legal interests are otherwise honored.²⁸⁴ Local educational agencies also must be attentive to the rights of noncustodial parents and provide them with equal access rights to the custodial parent, in the absence of a court order, statute, or other document that has revoked those rights.²⁸⁵ However, that same access should also be afforded to students, considering after all that the records do belong first and foremost to them.

A local policy might adopt a minimum age requirement at which students could exercise these access rights on a routine basis; however, COPPA attributes thirteen-year-olds with the maturity to make on-line decisions and that seems an appropriate age to start. Regardless, the local policymakers have to be cognizant that, at some point, mature minors may decide to limit parental access entirely. And there is clearly no parental access to certain medical information that is privileged or otherwise undisclosable pursuant to statute, such as the substance abuse records and medical matters for which mature minors can make their own decisions.

A local committee needs to look no farther than both the statutory and regulatory frameworks of FERPA and IDEA to follow a template within which to work for activating the access process. Within a reasonable time (and not more than forty-five days) of a request, an educational agency must allow parents and eligible students the opportunity to inspect and review the record.²⁸⁶ Both regulatory schema require the educational agency to respond to reasonable requests for interpretations and explanations, to provide copies if requested, and under IDEA, to allow a representative of the parent the same right to access.²⁸⁷ These rather straightforward requirements have been fairly adequately documented, with appropriate exemplars

283. 20 U.S.C. § 1232g(a)(1)(A) (Supp. II 2002).

284. See generally NAT'L COMM. FOR CITIZENS IN EDUC., STUDENTS, PARENT AND SCHOOL RECORDS 32-35 (1974) (discussing the common law traditions and precedents that grant parents the right to review their children's records unless contrary to state statute or regulation).

285. 34 C.F.R. § 99.4 (2005). Each state's position on the rights of noncustodial parents should be examined closely to account for the amount of access to which they are entitled. See, e.g., *Crowley v. McKinney*, 400 F.3d 965 (7th Cir. 2005) (holding that a noncustodial parent does not have a liberty interest in direct access to student records).

286. 34 C.F.R. §§ 99.10(b), 300.562(a).

287. *Id.* §§ 99.10, 300.562.

provided by the DOE.²⁸⁸ Similar procedures should be provided to students, with the same notice and rights as parents have to access to and disclosure of their own records.

The local committee also would do well to consult its school board attorney about access rights under HIPAA—separate access protocols and separate records under HIPAA's regulations would militate adhering to the exact language of the statute and regulations.²⁸⁹

Participation: A fair information system must also provide an individual with the right to amend inaccurate records. Again, FERPA and IDEA (through its incorporation of FERPA) lay out the skeletal groundwork for a local educational agency to provide an amendment process, at least for parents.²⁹⁰ A parent or eligible student may request an amendment²⁹¹ to which the agency must respond within a reasonable period of time.²⁹² An agency's refusal to amend triggers a hearing process.²⁹³ A local educational agency should therefore be attentive to providing appropriate hearing procedures.²⁹⁴ Other privacy statutes, such as HIPAA, have similar amendment procedures.²⁹⁵

4. Integrity/Security Principle²⁹⁶

Integrity: Self-policing local procedures and reviewing the retention of records is the best formula for a local policy in maintaining the

288. FORUM GUIDE, *supra* note 8, at 57–69.

289. 45 C.F.R. § 164.524 (2005); see MOORE & WALL, *supra* note 121, at 9.

290. *E.g.*, 20 U.S.C. § 1232g(a)(2) (Supp. II 2002); see also 5 U.S.C. § 552a(d)(2)–(4) (2000). The Privacy Act provides that the agency must respond within ten days of the request for amendment. *Id.* § 552a(d)(2).

291. 34 C.F.R. §§ 99.20(a), 300.567(a).

292. *Id.* §§ 99.20(b), 300.567(b).

293. *Id.* §§ 99.20(c), 99.21–22, 300.567(c), 300.568–569.

294. See, *e.g.*, RUSSELL SAGE FOUND., *supra* note 212, at 23–24. Such quasi-judicial procedure might also include an annual review for the continued retention of some materials. *Id.* The early HEW Report suggested the following:

Maintain procedures that (i) allow an individual who is the subject of data in the system to contest their accuracy, completeness, pertinence, and the necessity for retaining them; (ii) permit data to be corrected or amended when the individual to whom they pertain so requests; and (iii) assure, where there is disagreement with the individual about whether a correction or amendment should be made, that the individual's claim is noted and included in any subsequent disclosure or dissemination of the disputed data.

HEW REPORT, *supra* note 266, at xxvi, 63–64. For sample procedural forms, see FORUM GUIDE, *supra* note 8, at 67–69.

295. 45 C.F.R. § 164.526 (2005); see MOORE & WALL, *supra* note 121, at 9.

296. One of the major difficulties surrounding a governmental agency's misuse of information it has collected may be more a product of government culture rather than deliberate erroneous disclosure, a question of control of government rather than control of the information. One commentator posits four reasons to "blame" that government culture: (i) individual privacy is in tension with and perhaps contrary to the substantive goals of the agency; (ii) individuals are not good

integrity and accuracy of records. The first part of such procedures would require that the agency "[m]aintain data in the system with such accuracy, completeness, timeliness, and pertinence as is necessary to assure accuracy and fairness in any determination relating to an individual's qualifications, character, rights, opportunities, or benefits that may be made on the basis of such data."²⁹⁷ Such procedures would require staff training and periodic retraining in addition to systemic evaluations of recordkeeping procedures.²⁹⁸ As for the retention policies, an agency should regularly "[e]liminate data . . . when the data are no longer timely."²⁹⁹ Regular purging of outdated education information, particularly disciplinary records and information with a short shelf-life, would remove obsolete information from disclosure.³⁰⁰

Security: Whatever local policies an educational agency might adopt concerning the collection and disclosure of student information, there is very little discretion in the necessity for keeping the information secure.³⁰¹ However, none of the federal statutes that protect children's privacy even intimate at security measures for the information, except IDEA.³⁰² The most helpful suggestion for establishing a secur-

guardians of their own privacy rights; (iii) government activity is not "reliably motivated" to protect privacy and is difficult to "monitor"; and (iv) information is an item that is difficult to define legally and therefore difficult to corral. Lillian R. BeVier, *Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection*, 4 WM. & MARY BILL RTS. J. 455, 464 (1995). Furthermore, although the government agency is in the "business" of collecting information, the individual is usually not voluntarily giving the information. *Id.* at 469. At least psychologically, the government is prying for its own purposes and has difficulty perceiving that the citizen is an unwilling participant. The government agency does not necessarily perceive its two "hats." Educational institutions have been accused of being similarly torn between their own self-interests and those of the students. *See, e.g.*, PRIVACY REPORT, *supra* note 69, at 429.

297. HEW REPORT, *supra* note 266, at 56-57.

298. *Id.* at 57.

299. *Id.*

300. *Id.* IDEA requires that parents be notified when special education information is destroyed. 34 C.F.R. § 300.573 (2005).

301. RUSSELL SAGE FOUND., *supra* note 212, at 23-24.

302. The applicable regulation states:

(a) Each participating agency shall protect the confidentiality of personally identifiable information at collection, storage, disclosure, and destruction stages.

(b) One official at each participating agency shall assume responsibility for ensuring the confidentiality of any personally identifiable information.

(c) All persons collecting or using personally identifiable information must receive training or instruction regarding the State's policies and procedures under § 300.127 and 34 C.F.R. part 99.

(d) Each participating agency shall maintain, for public inspection, a current listing of the names and positions of those employees within the agency who may have access to personally identifiable information.

34 C.F.R. § 300.572.

ity system comes from the Privacy Act of 1974, which requires a federal agency to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records."³⁰³ Combining the generalities of the Privacy Act with the specifics of IDEA would most benefit any security policy created by a local educational agency.

With regard to technical and physical safeguards, federal computer databases that hold government information have specific security guidelines for agency information systems.³⁰⁴ Likewise, local educational agencies must keep their computer systems tamper-free.³⁰⁵ However, not all educational information is on a computer system. To the extent that there exist paper files of any kind—permanent records, medical records, student work-product, and the like—each local agency must designate a secure location for the material to which only authorized personnel have access. In addition, IDEA regulations require special confidentiality of special education records. Consequently, it makes sense to segregate the records of special education students from those of the general education population. This is particularly so because IDEA requires that the school maintain a list of those employees with access,³⁰⁶ which necessitates the local privacy policy's treatment of administrative safeguards.

Administrative safeguards in place under FERPA and IDEA already require that access logs be kept of student records, except access provided to parents and authorized school personnel.³⁰⁷ Consequently, IDEA requires that one school official be in charge of the security of IDEA records and further mandates that persons collecting

303. 5 U.S.C. § 552a(e)(10) (2000) ("[A]nd to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."). One example of such agency security protocol for health information is the Center for Disease Control. See CTR. FOR DISEASE CONTROL, SECURITY INFORMATION FOR NEDSS BASE SYSTEM STATES: A CHECKLIST FOR SECURITY PROTECTION (2002), http://www.cdc.gov/nedss/Security/Security_InfoNB_Sys_Sites_V01.pdf. The security measures for HIPAA are in HIPAA Security Requirements Matrix, 45 C.F.R. pt. 164, subpt. C (2005), available at <http://www.ihs.gov/AdminMngrResources/HIPAA/Docs/HIPAA%20Security%20Requirements%20Matrix%20v2.doc>. For general policies for the Department of Commerce and the Office of Management and Budget, see NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, RECOMMENDED SECURITY CONTROLS FOR FEDERAL INFORMATION SYSTEMS (2005), <http://csrc.ncsl.nist.gov/publications/nistpubs/800-53/SP800-53.pdf>.

304. Computer Security Act of 1987, 15 U.S.C. §§ 278g-3 to -4 (Supp. II 2002).

305. See, e.g., FORUM GUIDE, *supra* note 8, at 77-78; NAT'L FORUM ON EDUC. STATISTICS, WEAVING A SECURE WEB AROUND EDUCATION: A GUIDE TO TECHNOLOGY STANDARDS AND SECURITY (2003), <http://nces.ed.gov/pubs2003/secureweb>.

306. 34 C.F.R. § 300.572(d).

307. *Id.* §§ 99.32(d), 300.563. FERPA's access logs must also note who requested access but was refused. *Id.* § 99.32(a)(1).

and using IDEA information receive appropriate training.³⁰⁸ Having to designate such an individual for *all* education records—ideally an administrator—would not be that much more difficult.³⁰⁹

Unlike IDEA's logs, FERPA's logs do not require notation of access by external state and federal agencies with a legitimate educational interest—such as transferee school systems³¹⁰—or by agencies with funding or regulatory authority of schools—such as the Comptroller General, the DOE, and state educational agencies; organizations studying educational institutions for improving testing and instruction; and school accreditation organizations.³¹¹ Similarly congruent is the disclosure of records for financial aid applications.³¹² All these functions can be justified on the notion that they are routine uses of the materials for which the student and parent would not otherwise be notified because consent is not required and therefore access need not be noted.

All other “external” access by individuals, agencies, and others requesting or otherwise obtaining access should be listed on appropriate rosters.³¹³ Similarly, the access log should be used by local juvenile authorities if an information-sharing compact is in place, as discussed above.³¹⁴

308. *Id.* § 300.572.

309. *See, e.g.,* RUSSELL SAGE FOUND., *supra* note 212, at 23.

310. 20 U.S.C. § 1232g(b)(1)(B) (Supp. II 2002).

311. *Id.* § 1232g(b)(1)(C), (F)–(G).

312. *Id.* § 1232g(b)(1)(D).

313. *Id.* § 1232g(b)(4)(A) (“Each educational agency or institution shall maintain a record, kept with the education records of each student, which will indicate all individuals (other than those [with legitimate educational interests]), agencies, or organizations which have requested or obtained access to a student's education records maintained by such educational agency or institution, and which will indicate specifically the legitimate interest that each such person, agency, or organization has in obtaining this information.”). Under IDEA, “[e]ach participating agency shall keep a record of parties obtaining access to education records collected, maintained, or used under [IDEA] (except access by parents and authorized employees of the participating agency), including the name of the party, the date access was given, and the purpose for which the party is authorized to use the records.” 34 C.F.R. § 300.563. Similarly, “[e]ach participating agency shall maintain, for public inspection, a current listing of the names and positions of those employees within the agency who may have access to personally identifiable information.” *Id.* § 300.572(d).

314. Law enforcement authorities would not sign an access log because, legally, they would have been required to give direct notice to the affected student and parent. In the failure of that notice, such disclosures would have to be noted in the appropriate log.

Equally important are concerns about access by the public at large and the press in particular. Although any lengthy discussion of the press and children's privacy is beyond the scope of this Article, the Freedom of Information Act (“FOIA”) prohibits the disclosure of agency materials that are “personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.” 5 U.S.C. § 552a(b)(6) (2000). Clearly,

5. *Enforcement/Redress Principle*

Federal Enforcement/Redress: A local education agency has no leeway in altering the procedures afforded by the federal statutes for enforcement of its laws, regardless of their lack of efficacy. FERPA and, hence IDEA, provide procedures through the DOE's Family Policy Compliance Office ("FPCO")³¹⁵ for violations of FERPA. IDEA also provides similar complaint procedures through state departments of education.³¹⁶ For the time being, FERPA does not provide a private right of action while IDEA still does. As a consequence, general education students' only statutory recourse is a financial penalty against the educational agency that has a "policy or practice" of failing to comply with FERPA while special education students have more "personal" and litigable rights.

The other miscellaneous privacy acts also have varying remedies, both administrative and judicial. PPRA leaves enforcement and redress up to the discretion of the Secretary of Education,³¹⁷ although complaints are still directed to the FPCO.³¹⁸ On the other hand, under the Privacy Act of 1974, unauthorized disclosures of SSNs are subject to civil remedies against the educational agency³¹⁹ and criminal penalties against the employee who made the unlawful disclosure.³²⁰ The National School Lunch program imposes fines and imprisonment.³²¹ COPPA applies only to private-sector data collection so the enforcement mechanism is through the FTC,³²² but an educational agency is unlikely to get caught up in a FTC enforcement action against a private entity. And substance abuse legislation pro-

educational records are "similar files" under FOIA and exempt from release by the agency. *Dep't of Air Force v. Rose*, 425 U.S. 352, 376-77 (1976). The information is, after all, not a function of the school *qua* governmental agency but a collection of records of school as keeper of the records in a centralized location for educational information, making educational records even more divorced from the agency function than even personnel files. Personnel files are exempt from access by the public—or release by the government agency—because they contain information, the disclosure of which would constitute an invasion of privacy. *Id.* at 371-72; *Wayland v. NLRB*, 627 F. Supp. 1473, 1478 (M.D. Tenn. 1986). Such prosaic information such as place of birth and date of marriage are non-accessible under FOIA. *See, e.g., Barvick v. Cisneros*, 941 F. Supp. 1015, 1020 (D. Kan. 1996). So why in the world should third parties have access to student records of minors that contain personally identifiable information?

315. 34 C.F.R. §§ 99.60-67.

316. *Id.* §§ 300.575, .660-662.

317. 20 U.S.C. § 1232h(e).

318. *See* U.S. DEP'T OF EDUC., PROTECTION OF PUPIL RIGHTS AMENDMENT (PPRA), <http://www.ed.gov/policy/gen/guid/fpcopprra/index.html> (last visited May 15, 2006).

319. 5 U.S.C. § 552a(g) (2000).

320. *Id.* § 552a(i).

321. 42 U.S.C. § 1758(b)(2)(C)(v) (Supp. II 2002).

322. 15 U.S.C. § 6505(a) (2000).

vides for criminal fines of \$500 to \$5000 for violations reported to the local United States Attorney.³²³

This system of statutory violations does not, however, prevent a student from going straight to court for a privacy violation, under either common law invasion of privacy, state constitutions and statutes, or the United States Constitution. Because the only two realistic remedies are relatively minor—injunctive relief or minimal damages—something other than litigation should be considered by a local policy committee. Although not necessarily binding in effect, internal mediation procedures and/or hearing officers might alleviate the risks of incurring the only real penalty in these cases—significant attorney fees for both parties.

Local Compliance: Obviously, internal, administrative sanctions against personnel would be useful in any privacy policy, but they would have to be subject to applicable law. Indeed, HIPAA requires the imposition of internal personnel sanctions,³²⁴ but any such policy must comport with the applicable state statutes and collective bargaining agreements for any and all school officials. All this suggests that the local policy provide for adequate training of personnel on the use of personally identifiable information in whatever form.

The more important matter is recourse and redress against the local educational agency itself. FERPA and IDEA already require administrative hearing procedures for local agencies to follow in the event there is a controversy about amending an education record,³²⁵ and each local educational agency is required to have policies and procedures in place for the intricate due process requirements of IDEA.³²⁶ Hence, an administrative remedy might be a good starting place to iron out problems with privacy issues at least with regard to violations that occur at the local agency level. Although an administrative agency hearing is not going to award damages, it can issue enforceable orders concerning injunctive relief and other curative measures that would be more personal. Making mediation an op-

323. 42 C.F.R. §§ 2.4–.5 (2005).

324. 45 C.F.R. § 164.530(e)(1) (2005) (“A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart [Privacy of Individually Identifiable Health Information].”). HIPAA also requires an internal procedure for filing complaints involving noncompliance with policies and procedures. *Id.* § 164.530(d). Unfortunately, there does not seem to be any redress. *See* MOORE & WALL, *supra* note 121, at 1. However, that may only be because the transition periods expected for compliance with the new HIPAA regulations were extended to April 2004. *Id.* §§ 164.532, .534. The complaints must be kept on file for six years. *Id.* § 164.530(j). The Department of Health and Human Services monitors records to track compliance with HIPAA privacy rules. *Id.* § 164.502(a)(2).

325. 34 C.F.R. § 99.22 (2005).

326. *Id.* §§ 300.500–.517.

tion—as now provided in IDEA—would also cure the problem. That is not to say that damages might not come up for which a lawsuit might be filed. However, many of these privacy concerns are one-off propositions that can be easily cured in the less acrimonious atmosphere of an administrative hearing.³²⁷

Regardless of the content of a local privacy policy, modern day privacy concerns and modern technology require adherence to these fair information practices. To the extent that the federal legislation that purports to protect children fails to incorporate those principles, the local agencies are left with the burden of doing so. The FIPs' formats are fairly easy to follow, and many federal agencies use them. Any guidelines similar to those described above would be useful to any local policy committee.

V. CONCLUSION

The goal of any local drafting committee is to craft a policy that will adhere to constitutional principles while still maintaining a local flavor that will satisfy its constituencies, including parents and students. Congress has proved frustratingly unable to come up with a coherent package of informational privacy for schoolchildren but has legislated a minefield of requirements that a local educational agency ignores at its peril. As a result, local schools must learn to tread the middle ground to comply with federal mandates and salvage their federal funding while still complying with their duties under the Constitution.

In the alternative, many school administrators are simply ignorant of their duties and/or are ignorant of student informational privacy rights. Either way, bad law and good intentions can be a toxic combination. Coming up with a local privacy policy forces a local educational agency to educate itself about those duties and rights. This *lex-praxis* that simplifies that process should assist them in reaching their appropriate objectives.

327. In matters relating to unlawful disclosure by third parties, an educational agency is clearly not in a position to impose fines on third parties so recourse to the courts might be the best bet, for both the educational agency and the students. Students in particular might avail themselves of traditional avenues for striking the use of improperly disclosed education records in response to legal orders and subpoenas.